Министерство образования и науки Российской Федерации
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

А.Ж. АБДЕНОВ, Г.А. ДРОНОВА,
В.А.ТРУШИН

СОВРЕМЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Утверждено Редакционно-издательским советом университета
в качестве учебного пособия

НОВОСИБИРСК
2017

УДК 004.056:681.51(075.8)
А 139

Рецензенты:

канд. физ.-мат. наук, доцент кафедры комплексной защиты информации ОмГТУ *Данилова О.Т.*,

профессор, заведующий кафедрой информационной безопасности НГУЭиУ *Пестунова Т.М.*

Работа подготовлена на кафедре защиты информации для студентов IV курса АВТФ дневной формы обучения, обучающихся по направлению «Информационная безопасность» и специальности «Информационная безопасность автоматизированных систем»

Абденов А.Ж.

А 139 Современные системы управления информационной безопасностью: учебное пособие / А.Ж. Абденов, Г.А. Дронова, В.А. Трушин. – Новосибирск: Изд-во НГТУ, 2017. – 48 с.

ISBN 978-5-7782-3236-5

Предназначено для студентов, обучающихся по направлению «Информационная безопасность» и специальности «Информационная безопасность автоматизированных систем», а также может быть полезно при переподготовке руководителей подразделений и специалистов по информационной безопасности как коммерческих, так и государственных организаций.

УДК 004.056:681.51(075.8)

ISBN 978-5-7782-3236-5

1. ВВЕДЕНИЕ

Эффективное функционирование современных бизнес-процессов невозможно без качественных, своевременных, надежных средств, систем, сервисов информационных технологий (ИТ). Снижение или нарушение работоспособности, недостаточность или потеря функциональности компьютерных средств, систем, сервисов, блокирование, утрата конфиденциальности данных, искажение, уничтожение информационных активов могут привести к дезорганизации или снижению деловой активности, финансовым потерям, потере репутации компании, нанесению ущерба здоровью персонала, возникновению других видов прямого или косвенного ущерба. Деловая активность организаций критически зависит от безопасности информации.

Значительно усложняет ситуацию то, что бизнес стал венчурным (высокорискованным), перечень ИТ-рисков для бизнеса включает до шестисот риск-факторов, ИТ современных организаций базируется на многокомпонентной, масштабной инфраструктуре, интегрированной с сетями общего пользования. В ИТ активно применяются технологии виртуализации и облачного сервиса. Очевидно, что чем сложнее система, тем более она уязвима. Успешная реализация хотя бы одной уязвимости способна привести к длительному останову, выходу из строя ИТ-инфраструктуры, утрате критичных данных и, соответственно, к останову бизнеса в целом. Успешно противодействовать актуальным угрозам безопасности может только комплексная, эшелонированная, упреждающая система информационной безопасности (СИБ). Эффективность СИБ обеспечивается современной системой управления информационной безопасностью (СУИБ), основанной на «лучших практиках» и ориентированной на управление рисками информационной безопсности.

Наличие уязвимостей в компьютерных системах, разнообразие видов компьютерных атак, их непредсказуемый характер, территориальная и временная распределенность средств защиты сетевой инфра-

структуры приводит к тому, что в настоящее время для обеспечения безопасности компьютерных сетей и систем важное значение имеют технологии проактивной защиты информации, нацеленные на упреждение нарушений информационной безопасности и осуществляющих непрерывный мониторинг, управление безопасностью информации. В основе технологий проактивной защиты лежит своевременный, оперативный сбор данных и метаданных о событиях безопасности, фиксируемых в записях журналов аудита компьютерной инфраструктуры, хранение данных в специализированном хранилище и последующая обработка, включающая процедуры классификации, корреляции, моделирования, выработки предупреждений и решений по противодействию атакам, а также другие наиболее эффективные оперативные процедуры восстановления и надежное сохранение безопасности информации. Другим названием для информационной системы (ИС), реализующей мониторинг и управление безопасностью информации, является термин *система управления информацией и событиями безопасности* (Security Information and Events Management, SIEM) [1, 2].

Для хранения и манипулирования данными и метаданными предлагается построение репозитория (хранилище данных или метаданных) на принципах сервис-ориентированной архитектуры (*SOA*, англ. *service-oriented architecture*). Доступ к данным и к метаданным осуществляется с использованием веб-сервисов. В частности, в качестве хранилища можно использовать СУБД (система управления базами данных) Virtuoso компании Open Link Software, которая поддерживает функциональность как реляционной СУБД, так и хранилища триплетов.

В общем случае к репозиторию предъявляются следующие функциональные требования: хранение данных; хранение метаданных; возможность корректировки метаданных; управление данными на разных уровнях детализации; последовательный доступ к данным и метаданным, основанный на привилегиях; поддержка целостности и непротиворечивости данных и метаданных; поддержка многоверсионного управления. В целом репозиторий должен являться средством кроссплатформенной интеграции различных компонентов SIEM-системы. В качестве основы предлагается выбрать сервис-ориентированную архитектуру – модульный подход к разработке программного обеспечения, основанный на использовании распределённых, слабо связанных (англ. *loose coupling*) заменяемых компонентов, оснащённых стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам. Программные комплексы, разработанные в соот-

ветствии с сервис-ориентированной архитектурой, обычно реализуются как набор веб-служб, взаимодействующих по протоколу SOAP. SOAP (от англ. *Simple Object Access Protocol* – простой протокол доступа к объектам) – протокол обмена структурированными сообщениями в распределённой вычислительной среде. Архитектура SOA является инновационной идеей для распределенной информационной среды, которая объединяет воедино различные программные модули и приложения, основанные на хорошо определенных интерфейсах, обеспечивает их взаимодействие.

Обсуждение вопросов, возникающих в разрабатываемых SIEM-системах для сервисных информационных инфраструктур проводится в проекте MASSIF (MAnagement of Security Information and Event in Service Infrastructure – Управление информацией и событиями безопасности в инфраструктурах услуг) седьмой рамочной программы Европейского Союза [1]. Мы предполагаем, что одним из обсуждаемых вопросов в рамках проекта MASSIF должны быть вопросы наполнения и постоянного совершенствования отдельных узлов SIEM-системы возможностями решения задач классификации инцидентов, прогнозирования, фильтрации и оптимизации использования средств защиты ИР в компьютерной системе (КС) [3–6]. Для достижения поставленных целей SIEM-система должна обладать возможностью успешного решения следующего комплекса задач:

– сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников;

– обнаружения в режиме реального времени атак, нарушений критериев и политик безопасности;

– анализа и управления рисками в ИС на основе объективных и экспертных оценок [5];

– оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ИР;

– проведения расследований инцидентов;

– обнаружения расхождения результатов анализа критически важных ИР и бизнес-процессов с внутренними политиками информационной безопасности (ИБ) и последующее приведение их в соответствие друг с другом;

– принятия эффективных решений по защите информации [6];

– формирования отчетных документов.

Основными исходными данными, которые используются SIEM-системой для решения указанных задач являются записи различных

журналов аудита (logs), протоколирующие события в информационной инфраструктуре, называемые «событиями безопасности». Данные события отражают такие действия пользователей и программ, которые могут оказать влияние на ИБ. Из общего множества событий безопасности SIEM-система должна в режиме реального времени находить такие события безопасности, которые свидетельствуют об атаках или иных воздействиях, причем традиционные методы поиска такой информации достаточно трудоемки.

Для обнаружения, анализа и разрешения возникающих проблем по защите ИР, разработанные в европейских государствах SIEM-системы имеют архитектуру «агенты–хранилище данных–сервер приложений» [1–3, 7, 8]. Агенты выполняют сбор событий безопасности, их первоначальную обработку, нормализацию, классификацию и фильтрацию. Собранные, классифицированные, отфильтрованные информации о событиях безопасности поступают в репозиторий (хранилище данных в SIEM-системах), где они хранятся во внутреннем формате представления с целью последующего использования и анализа сервером приложений. Серверы приложений анализируют информацию, хранимую в репозитории и преобразуют ее для выработки предупреждений, других рекомендаций в режиме реального времени, а также управленческих решений по защите информации.

В перспективных SIEM-системах (т. е. в системах нового поколения) к числу расширений функциональных наполнений узлов SIEM-системы следует добавить анализ событий, инцидентов и их последствий, принятие интеллектуальных решений и визуализацию информации. Раскроем примерное содержание некоторых механизмов функциональных наполнений узлов по уровням иерархии SIEM-системы:

– нормализация означает приведение форматов записей журналов, собранных из различных источников к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки [2, 3, 8];

– фильтрация событий безопасности заключается в корректировке текущих оценок состояния защищенности ИР в КС и расчеты этих оценок на будущий интервал времени [9, 10];

– приоритезация определяет значимость и критичность событий безопасности на основании правил, определенных в системе [1, 7];

– корреляция делается для того, чтобы заметить появление соответствующих шаблонов событий, шаблонов отношений между переменными событиями, с тем чтобы оценить уровень безопасности кон-

тролируемой области и генерировать подробные отчеты безопасности [4, 9, 10];

– анализ событий, инцидентов и их последствий включают процедуры моделирования событий, атак и их последствий, анализа уязвимостей, оценок риска, прогнозирование и фильтрации оценок и инцидентов [11–15];

– система поддержки принятия решений (СППР) определяет выработку мер по оптимизации и реконфигурированию средств защиты с целью предотвращения атак на КС [2, 3];

– генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования [2, 3, 4].

В данной работе будут предложены и раскрыты некоторые элементы наполнения отдельных узлов SIEM-системы алгоритмами решения задач расчета риска на основе объективных и экспертных оценок, а также расчета оценок предсказания и фильтрации количества неблагоприятных событий (НС), величину ущерба и оптимизации использования средств защиты ИР в КС [5, 6, 8, 9, 14].

2. ЗАДАЧИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

2.1. ЗАДАЧА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современный бизнес[1] не мыслим без использования информационных технологий. Практически все сферы деловой активности информатизированы, что обеспечивает их максимально эффективное и динамичное развитие.

Деловая активность подразумевает использование или преобразование посредством соответствующих технологий неких ресурсов. Однако, как сами ресурсы, так и технологии имеют уязвимости, которые могут быть реализованы, с той или иной степенью вероятности, как внешними или внутренними злоумышленниками, так и природными (стихийными) или техногенными негативными факторами. Наличие уязвимостей в информационной сфере порождает риски информационной безопасности, которые, в случае их успешной реализации, способны нанести финансовые, репутационные и иные потери деятельности организации (рис. 1)[2], приводящие к нарушениям непрерывности бизнеса. Решение задачи по обеспечению непрерывности бизнеса существенно затруднено из-за того, что современный бизнес является повышенно венчурным (высокорискованным), ИТ-инфраструктура

[1] В данном учебном пособии под бизнесом понимается любая деловая активность, включая деятельность государственных организаций.

[2] Риск – это возможность того, что произойдет определенное неблагоприятное событие, имеющее свою цену (размер ожидаемого ущерба) и вероятность наступления. Риск информационной безопасности представляет собой возможность нарушения ИБ с негативными для организации последствиями.

существенно усложнена и не имеет четких границ, наблюдается масштабный, поливариантный рост угроз информационной безопасности (сложные технические сбои, увеличение числа человеческих ошибок, злоумышленные действия персонала, взлом и проникновение внешних злоумышленников, увеличению числа и сложности компьютерных вирусов, DDoS-атаки и др.).

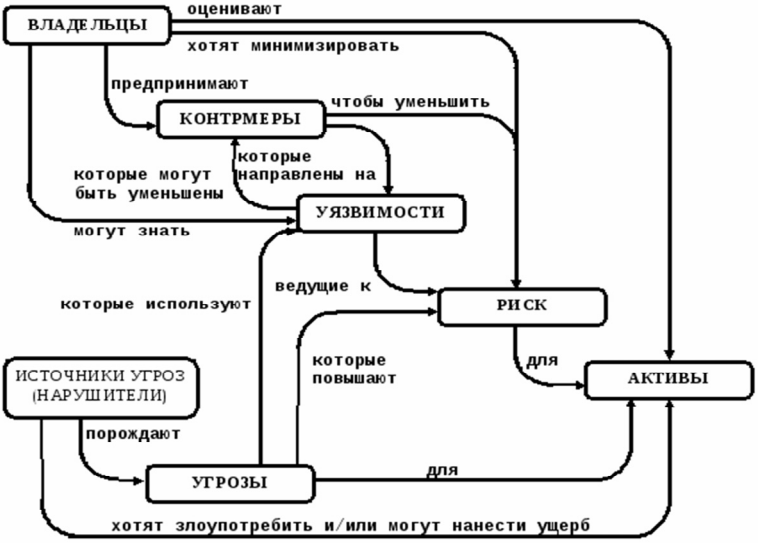

Рис. 1. Угрозы и риски

В целях снижения рисков прерывания деловой активности по причине реализации угроз ИТ в организации должна быть создана система информационной безопасности, которую можно определить как организованную совокупность специальных органов, служб, технических средств, методов и мероприятий, снижающих уязвимость информационных ресурсов, обеспечивающих целостность информации, доступность информации и информационных сервисов, препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Другими словами, главная стратегическая задача создания и совершенствования системы информационной безопасности заключается в *обеспечении непрерывности бизнеса посредством поддержания установленных уровней целостности, доступности и конфиденциальности для каждого актуального информационного ресурса.*

2.2. ЗАДАЧА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Эффективность системы информационной безопасности определяется наличием в организации соответствующей системы управления информационной безопасностью (СУИБ)[3].

Основными задачами СУИБ являются **организация, планирование, мотивация, контроль** действий в рамках СИБ, **сбор и оценка** результатов этих действий, **корректирующие воздействия** на СИБ. СУИБ должна функционировать на всех звеньях управленческой структуры организации (рис. 2).

Рис. 2. Система управления информационной безопасностью

Современная СУИБ обеспечивает объединение всех применяемых на предприятии технических и организационных мер в единый адекватный реальным угрозам управляемый комплекс, позволяющий достигать корпоративных целей информационной безопасности на уровне всего предприятия. СУИБ позволяет четко определить, как взаимосвязаны процессы и подсистемы ИБ, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования.

---

[3] СУИБ также именуется, как «система менеджмента информационной безопасности» (СМИБ).

3. ПАРАДИГМА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

3.1. РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КАК ПРОЦЕССА

Информационная безопасность оказывает прямое воздействие на деятельность компании в целом и, хотя относится к вспомогательным процессам, является одним из важнейших стратегических бизнес-процессов, поскольку направлена на обеспечение выполнения главных задач компании.

Информационная безопасность не приносит прибыли, но позволяет сохранить прибыльность других бизнес-процессов и реализуется согласно:

- бизнес-целям компании;
- условиям и принципам исполнения бизнес – процессов компании;
- требованиям национальных и международных стандартов.

3.2. ЦИКЛ ШУХАРТА–ДЕМИНГА

Создание СУИБ является частью большой бизнес-задачи по обеспечению информационной безопасности организации. Важной частью функционирования СУИБ является устойчивая повторяемость действий в рамках СУИБ и получение требуемых результатов этих действий.

Исходя из стандартного определения процесса, как устойчивой, целенаправленной совокупности взаимосвязанных действий, которые по определённой технологии преобразуют некие входы в заранее определенные выходы (материальная продукция или услуги, представляющие ценность для потребителя), можно сказать, что для комплексного решения задачи обеспечения информационной безопасности организации необходимо создавать СУИБ на основе т.н. **процессного подхода**.

В грубом приближении функционирование СУИБ организации можно представить в виде одного из бизнес-процессов - процесса «Управления информационной безопасностью». Поскольку задачу обеспечения непрерывности бизнеса организации, как уже отмечалось выше, невозможно решить одноразовым выполнением процесса «Управление информационной безопасностью», следовательно, данный процесс должен постоянно воспроизводиться сразу по окончании очередной своей итерации, т. е. процесс «Управление информационной безопасностью» должен быть **перманентным**.

Наиболее верным решением для обеспечения непрерывного улучшения процесса управления информационной безопасностью является функционирование его в цикле Шухарта-Деминга, в котором каждая итерация процесса состоит из т.н. PDCA-цикла (Plan-Do-Check-Act или Планируй-Делай-Проверяй-Действуй, рис. 3).

Рис. 3. Цикл PDCA

В процедуре **Планируй** (Plan) – производится установление целей и процессов, необходимых для достижения целей, планирование работ по достижению целей процесса и удовлетворения потребителя, планирование выделения и распределения необходимых ресурсов.

В процедуре **Делай** (Do) – реализуются запланированные действия.

В процедуре **Проверяй** (Check) – производится сбор информации и контроль результата на основе ключевых показателей эффективности (KPI), получившегося в ходе выполнения процесса, выявление и анализ отклонений, установление причин отклонений.

В процедуре **Действуй** (Act) – производится принятие мер по устранению причин отклонений от запланированного результата, изменения в планировании и распределении ресурсов.

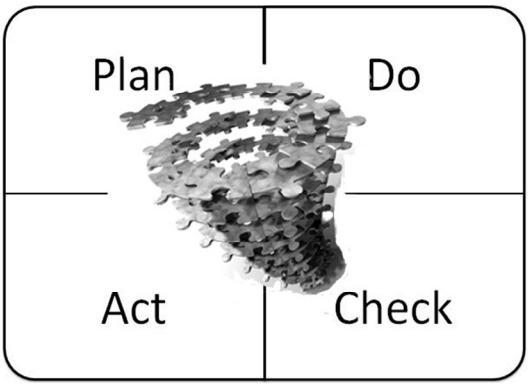

Рис. 4. Перманентность процесса в PDCA-цикле

Наличие в PDCA-цикле процедуры коррекции действий обуславливает качественное изменение процесса (переход на следующий уровень), поэтому процесс «Управления информационной безопасности» можно представить в виде непрерывной спирали (рис. 4).

3.3. ПРОЦЕССНЫЙ ПОДХОД В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Исходя из требований стандартов в процессе «Управление информационной безопасностью» можно выделить 20 процессов нижнего уровня таких как – «Управление логическим доступом», «Управление инцидентами», «Управление рисками» и т. д. Кроме того, каждый процесс ИБ в свою очередь состоит из набора процедур – например, процесс «Осведомленность и информирование» состоит из процедур «Первичный инструктаж по требованиям информационной безопасности», «Повышение уровня осведомленности персонала по вопросам информационной безопасности», «Тестирование уровня знаний персонала по вопросам ИБ», «Финальный инструктаж» и т. д.

Правильное построение СУИБ на основе процессного подхода подразумевает управление взаимосвязью этих процессов информационной безопасности. Суть процессного подхода можно пояснить следующим примером: для обеспечения непрерывного функционирования бизнеса необходимо иметь план обработки рисков. План обработки рисков в части защиты информации – это результат работы процесса ИБ «Управле-

ние рисками». Т. е. в организации должны быть разработаны, введены в эксплуатацию и давать правильные результаты, следующие процедуры процесса ИБ «Управление рисками» – «Инвентаризация и категорирование информационных ресурсов», «Обнаружение уязвимостей информационных ресурсов», «Анализ и оценка рисков», «Обработка рисков» и др. Однако, наличие даже самых совершенных мер по снижению рисков информационной безопасности не может полностью предотвратить возникновение в информационной среде событий, несущих угрозу бизнесу (инцидентов ИБ). Следовательно, должен функционировать процесс ИБ «Управление инцидентами», который в свою очередь приведет к необходимости внедрения процесса «Управление проблемами».

Кроме того, для функционирования эффективной СУИБ, процессам ИБ необходимо тесное взаимодействие с ИТ-процессами организации (как минимум с восемнадцатью базовыми (согласно ITIL) или тридцатью семью, согласно CobiT v.5, ИТ-процессами).

3.4. ДОКУМЕНТИРОВАННОСТЬ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Следующей важной составляющей в создании СУИБ организации является построение системы на основе знаний принципов практической реализации требований законодательства (ФЗ-152, ФЗ-149 и т. д.), современных международных и отечественных стандартов в области информационной безопасности (семейства стандартов ISO 27000, NIST SP 800, СТО БР ИББС и т. д.), информационных технологий (ISO 20000, ITIL), ИТ-аудита (CobIT), отраслевых требований. Положения стандартов, например, позволяют разбить процесс «Управление информационной безопасностью» на составляющие его процессы низкого уровня, обеспечивающие выполнение набора требований определенной тематики – например обеспечение физической безопасности ИТ-инфраструктуры и т. д.

Исходя из главной стратегической задачи информационной безопасности система управления информационной безопасностью должна:

- иметь достаточные уровни зрелости процессов, отвечающие установленным бизнесом организации[4] требованиям;
- функционировать в непрерывном цикле.

[4] Изучение способов достижения указанной цели не входит в данный курс.

Одним из элементов достижения указанных целей является наличие полезных, эффективных документов, описывающих каждый процесс или процедуру ИБ. Наиболее рациональная иерархия комплекта документов по ИБ, сложившаяся в настоящее время, представлена на рис. 5.

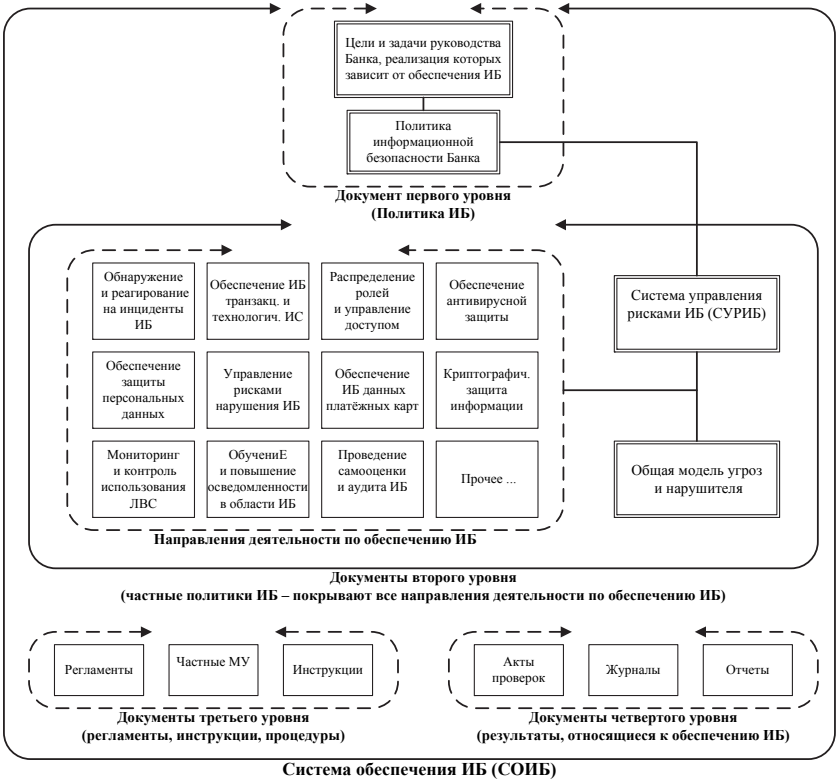

Рис. 5. Иерархия документов системы информационной безопасности

Документы первого уровня, определяют высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенные для организации в целом (настоящий документ, Политика ИБ).

Документы второго уровня (частные политики ИБ), детализируют положения Политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации.

Документы третьего уровня, содержат положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) обеспечения ИБ, содержащие правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ, в рамках бизнес-процессов, используемых в организации, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых бизнес-процессах (технические задания, регламенты, порядки, инструкции, процедуры, положения, правила и др.).

Документы четвертого уровня, содержат свидетельства выполненной деятельности по обеспечению ИБ, отражающие достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ организации.

3.5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В рамках процессов ИБ, функционирующих в системе управления информационной безопасностью, выполняется определенный перечень мероприятий, направленных на поддержание установленных в организации требований ИБ, а также функционирует ряд технических систем защиты информации. В совокупности этот перечень называется организационно-техническими требованиями по ИБ. К организационным мероприятиям по ИБ относятся различные инструктажи, повышение уровня осведомленности сотрудников, предоставление доступа к информационным ресурсам на основании согласованных заявок, периодическая проверка (аудит) процессов ИБ. Наряду с организационными мерами в организации должны применяться различные технические системы защиты информации – антивирусной защиты, защиты от несанкционированного доступа, обнаружения и предотвращения вторжений и т. д.

В недалеком прошлом достаточным являлось проведение периодического (например, раз в год) выборочного контроля выполнения мероприятий по ИБ. Однако, с течением времени, в связи с указанными выше причинами (венчурность бизнеса, усложнение ИТ-инфраструктуры, развитие средств и методов атак на информационные ресурсы и т. д.) периодический, выборочный контроль защищенности информационных ресурсов перестал отвечать современным ИТ-угрозам. Современная

СУИБ в настоящее время должна выполнять следующие требования – максимальный охват области контроля (идеальный вариант – 100 %), контроль должен быть непрерывным (аудит смещается в область непрерывного мониторинга), реагирование на угрозы в он-лайн режиме, проактивность защитных мер. Выполнение новых требований к СУИБ ведет к необходимости сбора, обработки, анализу огромного объема информации, точной оценке рисков, мгновенной оценке и принятию адекватного решения по мерам противодействия возникающим угрозам, применение систем искусственного интеллекта при анализе потоков информации. В настоящее время техническим инструментарием, позволяющим реализовывать вышеуказанные функции, является класс SIEM-систем.

4. ОЦЕНИВАНИЕ РИСКА В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ОБЪЕКТИВНЫХ ОЦЕНОК ДЛЯ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПРИ РАСЧЕТЕ ЭКСПЕРТНЫХ ОЦЕНОК

Основанный на рисках подход к оценке потенциального ущерба от атак нарушителей и выбору мер для его минимизации получил название «Управление рисками». Под «управлением рисками» подразумевается полный комплекс алгоритмов и мероприятий из ряда выполняемых последовательно процессов, что соответствует существующим международным стандартам и практике управления рисками на предприятиях [13, 14]: идентификация рисков, анализ рисков, принятие рисков, мониторинг и пересмотр. В существующих методиках управления рисками их идентификация осуществляется различными методами такими, как командные «мозговые штурмы», анализ архитектуры системы защиты информационных ресурсов (ИР), операционное моделирование, анализ сценариев, исследования HAZOP (HAZard and OPerability studies). HAZOP – это признанный лидер при анализе рисков на особо опасных объектах с катастрофичными последствиями [12]. На современном этапе одна из эффективных методик управления рисками основана на экспертных оценках [13].

Основанием расчета и анализа рисков являются статистические данные из репозитория SIEM-системы, собранные в процессе идентификации рисков, а результаты работы системного аналитика используются лицами или процессами из соответствующих узлов SIEM-систем, принимающими решения в СППР [13]. В настоящее время модели анализа и оценки рисков проходят стадию развития [14], которые рассматривают управление рисками как принятие решений в условиях неопределенности, а количественные показатели риска – как критерии принятия альтернативных или взаимодополняющих решений в процессе какой-либо деятельности.

Оценки риска рассчитываются в зависимости от вероятности реализации НС в ИС. Различают объективные и субъективные вероятности наступления НС. Оценка объективных вероятностей наступления НС – одна из важных задач в алгоритме расчета оценок риска. При этом использование этих объективных оценок для повышения эффективности и достоверности расчетов экспертных оценок риска в ИС предприятия является важной задачей в методике расчета оценок потенциального ущерба от атак нарушителей.

4.1. АЛГОРИТМ РАСЧЕТА ОБЪЕКТИВНОЙ ВЕРОЯТНОСТИ РЕАЛИЗАЦИЙ НЕБЛАГОПРИЯТНЫХ СОБЫТИЙ В КОМПЬЮТЕРНОЙ СИСТЕМЕ

Для эффективного анализа НС воздействующих на ИР в ИС, необходимо предварительно решить некоторые задачи классификации и корреляции [4, 10]. В частности, для построения математической модели в форме моделей пространства состояний (ПС) [8, 9] с целью оценивания состояния защищенности ИР в ИС, в первую очередь, необходимо определить уровень «зрелости» предприятия с точки зрения обеспечения ИБ. Для этого можно воспользоваться классификацией, предложенной специалистами компании Gartner[5], которая подразумевает четыре уровня «зрелости» [15].

Нулевой уровень ($i = 0$):

- ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ;
- финансирование отсутствует;
- ИБ на примитивном уровне реализуется штатными средствами операционных систем, систем управления базами данных и приложений.

Первый уровень ($i = 1$):

- ИБ рассматривается руководством как чисто «техническая» проблема, отсутствует единая программа (концепция ИБ, политика) развития систем обеспечения информационной безопасности (СУИБ) предприятия или организации;

[5] Gartner – исследовательская и консалтинговая компания, специализирующаяся на рынках информационных технологий. Официальный сайт: www.gartner.com.

- финансирование ведется в рамках общего бюджета на информационные технологии;
- ИБ реализуется средствами нулевого уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (Virtual Private Network – построения виртуальных частных сетей), т. е. традиционные средства защиты.

Второй уровень ($i = 2$; $u = 2$):

- ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для производственных процессов, есть утвержденная руководством программа развития СУИБ компании;
- финансирование ведется в рамках отдельного бюджета;
- ИБ реализуется средствами первого уровня плюс средства усиленной аутентификации, средства анализа почтовых сообщений и web-контента, IDS (Intrusion Detection System – системы обнаружения вторжений), средства анализа защищенности, SSO (Single Sign On – средства однократной аутентификации), PKI (Public Key Infrastructure – инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика ИБ, положения, процедуры, регламенты и руководства).

Третий уровень ($i = 3$; $u = 1$):

- ИБ является частью корпоративной культуры, назначен CISA (Certified Information Systems Auditor – старший администратор по вопросам обеспечения ИБ);
- финансирование ведется в рамках отдельного бюджета;
- ИБ реализуется средствами второго уровня плюс системы управления ИБ, CSIRT (Computer Security Incident Response Team – группа реагирования на инциденты нарушения ИБ), SLA (Service Level Agreement – соглашение об уровне сервиса).

Таким образом, специалисты по ИБ или экспертная группа на конкретном предприятии могут зафиксировать значение входного управляющего сигнала, отнеся свою компанию к тому или иному уровню «зрелости» в соответствии с представленной классификацией. Значение входного управляющего сигнала $u(t)$ может быть задано также компетентными специалистами, которые учтут род деятельности предприятия, количество сотрудников и прочие данные, влияющие на систему ИБ.

Каждый зафиксированный инцидент, должен пройти процедуру классификации с целью определения вида НС и помещения зафикси-

рованного инцидента в определенный класс для последующих процедур обработки.

Далее необходимо осуществить процедуру классификации в зависимости от количества компьютерных рабочих мест (КРМ). Такая классификация необходима при оптимизации выбора средств защиты ИР в ИС. При этом классификация очень сильно влияет на оценку определения уровня «зрелости» предприятия или организации. Количественные интервалы относительно КРМ должны определяться специалистами по ИБ, которые знакомы со статистической информацией, хранящейся в репозиториях SIEM-систем.

После всех процедур относительно решения задач классификации и корреляции можно переходить к расчету объективных оценок с целью повышения объективной информативности для принятия решений при расчете субъективных оценок в окончательной процедуре оценивания риска. В работе [5] была предложена одна версия методики расчета объективной вероятности реализаций НС в КС. В данной работе эта методика дополнена вариантом условия учета взаимной корреляции шумов динамики поведения исследуемого объекта и шумов измерительной системы при расчете оценок предсказания и фильтрации количества НС и соответствующих оценок ущерба.

Из списка множества существующих видов НС, имеющихся в репозитории SIEM-системы, выделяются существенное подмножество видов НС, приводящих к ощутимому нарушению безопасности ИР в КС. Это подмножество обозначим через $O = \left\{ O_{i_1}, O_{i_2}, \ldots, O_{i_m} \right\}$, например, O_{i_1} – вид НС относительно нарушения запуска отдельных узлов КС; O_{i_2} – вид НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т. д.

После построения подмножества O, переходим к анализу свойств элементов подмножества на основе количественных показателей НС и соответствующей величины ущерба, имевшей место в прошлом. Математическое ожидание ущерба, вызываемого i-м НС за время ΔT (например, 1 месяц), можно представить формулой:

$$e(O_i, \Delta T) = M\left[e(O_i) \cdot f_i \right], i = \overline{1,m}, \qquad (1)$$

где $e(O_i)$ – случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i – случайная величина количества НС

i-го вида за время ΔT; m – общее количество всех видов уже свершившихся НС i-ого вида.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = M\left[e(O_i)\right] \cdot M\left[f_i\right], \quad i = \overline{1,m}, \tag{2}$$

а ущерб для всего множества существенных НС будет определяться с помощью соотношения

$$E(O, \Delta T) = \sum_{i=1}^{m} M\left[e(O_i)\right] M\left[f_i\right]. \tag{3}$$

Алгоритм 1

Шаг 1.1. Для простоты будем рассматривать лишь один вид НС, например, зафиксируем конкретное значение $i = 1$. Далее, количественные показатели НС, например, за μ лет сведем в табл. 1:

Таблица 1

Количественные показатели НС $\left(f_i^{(j)}\right)$, произошедших в течение последних μ лет по месяцам

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$f_1^{(1)}$	$f_2^{(1)}$	$f_3^{(1)}$	$f_4^{(1)}$	$f_5^{(1)}$	$f_6^{(1)}$	$f_7^{(1)}$	$f_{18}^{(1)}$	$f_9^{(1)}$	$f_{10}^{(1)}$	$f_{11}^{(1)}$	$f_{12}^{(1)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$f_1^{(\mu)}$	$f_2^{(\mu)}$	$f_3^{(\mu)}$	$f_4^{(\mu)}$	$f_5^{(\mu)}$	$f_6^{(\mu)}$	$f_7^{(\mu)}$	$f_8^{(\mu)}$	$f_9^{(\mu)}$	$f_{10}^{(\mu)}$	$f_{11}^{(\mu)}$	$f_{12}^{(\mu)}$

где – $f_i^{(j)}$, $j = \overline{1,\mu}$, μ – количество лет, $t = \overline{1,12}$, t – номер месяца в году.

Шаг 1.2. Исходя из данных табл. 1, с помощью формулы (4) можно получить одну строку данных усредненных помесячных количественных значений НС по столбцам:

$$f_t^{\text{уср}} = \sum_{i=1}^{\mu} f_t^{(i)} / \mu, \; t = \overline{1,12}. \tag{4}$$

Аналогичные таблицы желательно построить относительно других существенных видов НС.

Шаг 1.3. Для дальнейших расчетов необходимо подготовить данные, которые являются данными округленными до целого относительно данных таблицы, полученные по формуле (4) (см. табл. 2).

Таблица 2

Усредненная строка количественных показателей произошедших НС, округленных до целого относительно данных таблицы, полученные по формуле (4)

t	1	2	3	4	5	6	7	8	9	10	11	12
$f_{\text{ц}t}^{\text{уср}}$	$f_{\text{ц}1}$	$f_{\text{ц}2}$	$f_{\text{ц}3}$	$f_{\text{ц}4}$	$f_{\text{ц}5}$	$f_{\text{ц}6}$	$f_{\text{ц}7}$	$f_{\text{ц}8}$	$f_{\text{ц}9}$	$f_{\text{ц}10}$	$f_{\text{ц}11}$	$f_{\text{ц}12}$

Шаг 1.4. Применительно к усредненным данным (см. табл. 2) можно построить математическую модель в форме пространства состояний (ПС) по методике, изложенной в [5]:

$$x(t+1) = a \cdot x(t) + b + w(t), \quad x(1) = \overline{x}_1, \tag{5}$$

$$f^{\text{уср}}(t+1) = x(t+1) + v(t+1), \quad t = \overline{1, N-1}. \tag{6}$$

где $x(t)$ – истинное количество фиксированного вида НС, произошедших в течение месяца t; $w(t)$ – белое гауссовское ненаблюдаемое воздействие на зафиксированный вид НС в момент времени t с нулевым математическим ожиданием и неизвестной дисперсией Q; $x(1)$ – гауссовская величина, отражающая количество НС в начальный в момент времени $t = 1$ с математическим ожиданием $\overline{x}_1$ и неизвестной дисперсией $P(1)$; a, b – неизвестные коэффициенты в модели динамики (5); t – номер месяца в году; $N = 12$ – число месяцев в году; $f_t^{\text{уср}} = f^{\text{уср}}(t)$ – наблюдаемое случайное количество НС в течение месяца t (данные из репозитория SIEM-системы или из журнала наблюдений предприятия); $v(t)$ – белая гауссовская последовательность ошибок наблюдений относительно количества НС в течение каждого месяца с нулевым математическим ожиданием и неизвестной дисперсией R.

На данном шаге требуется оценить все дисперсии, связанные с шумами модели динамики $\hat{Q}$ и шумом величины начального состояния $\hat{P}(1)$, шумами измерительной системы $\hat{R}$ на основе выхода данных наблюдений и рекуррентных формул, которые приведены в работе [5].

Шаг 1.5. Оценки коэффициентов $\hat{a}, \hat{b}$ в модели динамики (5) можно рассчитать с помощью метода наименьших квадратов (МНК) на основе (возможно отфильтрованных от шумов) данных наблюдений $\left\{x(t) \approx f^{\text{уср}}(t), t = \overline{1, N}\right\}$.

Шаг 1.6. Построенная модель (5), (6) позволит получить наиболее достоверные оценки количества НС с учетом условий взаимной независимости шумов динамики поведения и измерителя [5] или случай взаимной их коррелированности [9] (возможны и другие случаи, например случай коррелированности данных выхода измерительной системы), относительно каждого месяца в виде оценок фильтрации за последующий, например, $(\mu + 1)$ год (в режиме реального времени с помощью уравнений фильтра Калмана). Полученные оценки фильтрации должны быть округлены до ближайшего целого.

Шаг 1.7. Оценки фильтрации за 12 месяцев $(\mu + 1)$ года (рассчитанные на основе данных реальных наблюдений и оценок предсказаний) позволят рассчитать объективные вероятностные оценки реализаций НС. Например, предлагается следующая процедура расчета вероятности для конкретного вида НС.

Пусть нас интересует вероятность появления НС в каждом месяце предыдущего μ-го года. Для этого подсчитывается общее суммарное количество (для усредненного количества) НС оценок фильтрации в течение всего μ-года ($F^{(\mu)}$), а затем фильтрационная оценка количества НС в течение каждого месяца ($f^{(\mu)}(t)$) делится на общую суммарную оценку фильтрационных оценок количества НС ($F^{(\mu)}$) в течение одного μ-года, которая определяется по формуле:

$$p^{(\mu)}(t) = f^{(\mu)}(t) / F^{(\mu)}, \quad t = \overline{1, 12}, \tag{7}$$

где $p_t^{(\mu)} = p^{(\mu)}(t)$ – объективная вероятность реализации конкретного вида НС в течение каждого месяца μ-года и всех 12 месяцев (табл. 3). При этом для μ-го года будем иметь:

$$\sum_{t=1}^{12} p^{(\mu)}(t) = 1, \quad \mu = 4, 5, \ldots.$$

Таблица 3

Объективные вероятности $\left(p_t^{(\mu)}\right)$ реализаций конкретного вида НС в течение μ-го года

t	1	2	3	4	5	6	7	8	9	10	11	12
$p_t^{(\mu)}$	$p_1^{(\mu)}$	$p_2^{(\mu)}$	$p_3^{(\mu)}$	$p_4^{(\mu)}$	$p_5^{(\mu)}$	$p_6^{(\mu)}$	$p_7^{(\mu)}$	$p_8^{(\mu)}$	$p_9^{(\mu)}$	$p_{10}^{(\mu)}$	$p_{11}^{(\mu)}$	$p_{12}^{(\mu)}$

где – $p_t^{(\mu)}$, $t = \overline{1, 12}$, μ-ый – год.

Алгоритм 1, например, апробирован на тестовом примере при условии взаимной независимости шумов динамики поведения и измерителя [5]. В данной работе алгоритм 1 реализован для случая взаимно-коррелированных шумов объекта и измерителя [9] относительно модели в форме ПС вида (5), (6).

Результаты расчетов алгоритма 1 фиксируются в виде отдельной строки таблицы объективных оценок реализаций НС в КС для каждого вида из подмножества существенных видов НС $O = \left\{O_i, i = \overline{1, m}\right\}$, приводящих к ощутимому нарушению безопасности ИР в КС.

4.2. ОБЪЕКТИВНАЯ СТОИМОСТНАЯ ОЦЕНКА ПРЕДСКАЗАНИЯ ВЕЛИЧИНЫ УЩЕРБА ОТ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИР

Алгоритм 2

Шаг 2.1. Пусть $O = \left\{O_i, i = \overline{1, m}\right\}$ – множество существенных видов НС, приводящих к нарушению безопасности ИР. В п. 1.1. данной работы была предложена и кратко описана процедура расчета оценки помесячной объективной вероятности количества нарушений определенного

вида атаки на ИР в ИС предприятия. Предположим далее, что в отделе информационной безопасности (ИБ) предприятия или в репозитории SIEM-системы имеется статистика относительно ежемесячной оценки ущерба, которая соответствует ежемесячному количеству нарушений ИБ конкретного i-го вида атаки, т. е. значениям данных табл. 1 соответствуют значения данных табл. 4. Пусть, например, $i = 1$.

Таблица 4

Количественные ежемесячные показатели ущерба $\left(S_t^{(j)}\right)$ от нарушений ИБ в зависимости от i-го вида атаки

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$S_1^{(1)}$	$S_2^{(1)}$	$S_3^{(1)}$	$S_4^{(1)}$	$S_5^{(1)}$	$S_6^{(1)}$	$S_7^{(1)}$	$S_8^{(1)}$	$S_9^{(1)}$	$S_{10}^{(1)}$	$S_{11}^{(1)}$	$S_{12}^{(1)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

где – $S_t^{(j)}$, $j = \overline{1, \mu}$, μ – количество лет, $t = \overline{1, 12}$, t – номер месяца в году.

Шаг 2.2. Заметим, что не всегда ежемесячные показатели ущерба прямо пропорциональны количеству произошедших НС. Тем не менее, на основе данных табл. 4 можно построить линейную модель в форме ПС, которая будет соответствовать усредненным данным наблюдений рассчитанным по столбцам относительно данных табл. 4. Элементы строки усредненных данных вычисляются с помощью соотношения (8) и могут быть сохранены в таблице.

$$s_t^{(y)} = \left(\sum_{t=1}^{\mu} S_t^{(\mu)} \right) \Big/ \mu, \; t = \overline{1, 12}. \tag{8}$$

Шаг 2.3. На основе строки усредненных данных $\left\{ s_t^{(y)}, \; t = \overline{1, 12} \right\}$ по алгоритму, описанный в работах [3] можно построить линейную модель в форме ПС вида

$$s(t+1) = \hat{c} \cdot s(t) + \hat{d} + w(t), \quad s(0) = s_0, \quad t = \overline{0, 11}, \tag{9}$$

$$s^y(t+1) = s(t+1) + v(t+1), \quad t = \overline{0, 11}. \tag{10}$$

При этом сначала на основе строки усредненных данных соответствующих таблице ущербов рассчитываются оценки неизвестных дисперсий шумов модели вида (9), (10), а именно оценки дисперсий $\hat{Q}$, $\hat{R}$, $\hat{P}(1)$ на основе рекуррентных формул, которые предложены и описаны в работе [5].

Шаг 2.4. Далее рассчитываем коэффициенты $\hat{c}, \hat{d}$ модели динамики (9) с помощью МНК на основе данных из таблицы строки усредненных данных.

Шаг 2.5. Предположим, что мы располагаем данными наблюдений количественных показателей ущерба (например, из репозитария SIEM-системы), нанесенных ИР предприятия в $(\mu+1)$ году (см. табл. 5):

Таблица 5

Ежемесячные количественные показатели ущерба от нарушений ИБ в зависимости от i-го вида атаки в $(\mu+1)$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$S_t^{(\mu)}$	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

где – $S_t^{(\mu)}$, $t=\overline{1,12}$, $\mu=\mu+1$-ый – год.

Используя уравнения фильтра Калмана и данные табл. 5, получим последовательность наиболее значимых оценок фильтрации $\left\{\hat{s}(t\mid t), t=\overline{1,12}\right\}$ относительно ежемесячных более достоверных количественных показателей нанесенного ущерба, представленных в виде строки таблицы ежемесячных количественных показателей оценок фильтрации нанесенного ущерба в $(\mu+1)$ году.

Шаг 2.6. Используя округленные до ближайших целых чисел данные, оценок фильтрации относительно количественных показателей, свершившихся НС в течение $(\mu+1)$ года по месяцам и данные табл. 5 относительно оценок фильтрации как количественных показателей ущерба, нанесенных на ИР предприятия в $(\mu+1)$ году, можно получить усредненный ущерб нанесенных от единичного случая свершившегося НС $\left\{e(t),\ t=\overline{1,12}\right\}$. Для этого необходимо данные строки

табл. 5 разделить на соответствующие данные из табл. 2, округленные до целого, элементы строки данных количества реализации НС. Расчетные данные можно свести в табл. 6.

Таблица 6

Усредненный нанесенный ущерб от единичного случая свершившегося НС

t	1	2	3	4	5	6	7	8	9	10	11	12
$e(t)$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}

Шаг 2.7. Предсказывая количество НС (f_i^{pre}) i-го вида с помощью соответствующей модели в форме ПС (5), (6) и соответствующего усредненного ущерба от единичного случая свершившегося НС (т. е. по данным таблицы 6), можно получить оценку предсказания величины ущерба, которая будет нанесена предприятию в t- ый месяц $(\mu + 2)$ (текущего) года.

Алгоритм 2, например, апробирован на тестовом примере при условии взаимной независимости шумов динамики поведения и измерителя [5]. В данной работе алгоритм 2 реализован для случая взаимно-коррелированных шумов объекта и измерителя [9] относительно модели в форме ПС вида (9, 10).

Результаты расчетов алгоритма 2 фиксируются в виде отдельной строки таблицы объективных оценок предсказания величины ущерба в зависимости от соответствующих оценок реализаций НС в КС для каждого вида НС из подмножества существенных видов НС $O = \{O_i, i = \overline{1, m}\}$, приводящих к ощутимому нарушению безопасности ИР в КС.

Наконец, вся экспертная группа перед выставлением своих экспертных оценок, по различным семействам контролей безопасности [13], должна быть ознакомлена с результатами таблицы объективных оценок реализаций НС в КС и соответствующей таблицы объективных оценок предсказания величины ущерба для каждого вида НС из подмножества существенных видов НС $O = \{O_i, i = \overline{1, m}\}$, приводящих к ощутимому нарушению безопасности ИР в КС.

4.3. ГРУППЫ КОНТРОЛЕЙ БЕЗОПАСНОСТИ

Меры безопасности (альтернативное название – «контроли безопасности»), возможно применяемые для ИБ в ИС предприятий, которые можно поделить на три основные группы: технические, операционные и управленческие [13]. Группы в свою очередь разбиваются на семейства. Перечислены эти контроли безопасности в стандарте [16].

В группу управленческих контролей входят меры безопасности для ИС, которые используются при управлении рисками для ИБ ИС. Группа содержит пять семейств контролей [13, 16]. В группу операционных контролей входят меры безопасности для ИС, которые прежде всего, реализуются и выполняются людьми. В группу входят 9 семейств контролей. В группу технических контролей входят меры безопасности для ИС, которые, прежде всего, реализуются и выполняются через действия в аппаратных средствах, программном обеспечении системы. В группу входят четыре семейства контролей [13, 16].

Эксперты могут быть включены в группу с различной профессиональной подготовкой, например: технической, финансовой, инженерной и управленческой, со своими собственными индивидуальными восприятиями, отношениями и побуждениями в определении ущерба от количества реализованных НС. Поэтому, перед началом расчета величины риска в ИС предприятия на основе экспертных оценок необходимо всем экспертам ознакомиться с результатами: таблицы объективных оценок реализаций НС в КС и соответствующей таблицы объективных оценок предсказания величины ущерба для каждого вида НС из подмножества существенных видов НС $O = \left\{ O_i, i = \overline{1, m} \right\}$, приводящих к ощутимому нарушению безопасности ИР в КС. После знакомства с результатами этих двух таблиц объективных оценок, по всем видам существенных НС, каждый эксперт из группы выставляет свои экспертные оценки и на основе этих оценок проводят расчет оценок риска по всем ИС предприятия.

Например, пусть на предприятии, для которого мы оцениваем риски, существует три ИС: ИС-1, ИС-2, ИС-3. Экспертами после ознакомления с результатами объективных оценок были обнаружены определенные уязвимости и угрозы, относящиеся к различным семействам контролей. Далее были проведены расчеты оценок риска на основе экспертных оценок по методике, описанной в работе [13]. Методика расчетов риска для всех трех ИС была апробирована на тестовых данных. Результаты численных расчетов приведены в работе [5].

После ранжирования ИС по уровню риска в порядке убывания были получены следующие расчетные данные (см. табл. 7).

Таблица 7

Ранги информационных систем

Информационная система	ИС-2	ИС-3	ИС-1
Уровень риска	0,453	0,446	0,410

Из табл. 7 видно, что ИС-2 получает самый высокий уровень риска. Значит, вероятность реализации угроз и ущерб для этой системы больше, чем для остальных систем. Поэтому руководителям организации, в первую очередь, необходимо обратить внимание на безопасность ИС-2. Более подробную и детальную рекомендации можно получить от соответствующих узлов SIEM-систем.

4.4. АЛГОРИТМ ФИЛЬТРА КАЛМАНА. СЛУЧАЙ ВЗАИМНО-КОРРЕЛИРОВАННЫХ ШУМОВ ДИНАМИКИ И ИЗМЕРИТЕЛЯ

Выше было отмечено примерное содержание основных механизмов по уровням иерархии SIEM-системы: нормализация означает приведение форматов записей журналов, собранных из различных источников к внутреннему формату, которые затем будут использоваться в последующей обработке; корреляция разнородных событий; анализ событий, инцидентов и их последствий, включающая процедуры моделирования событий, анализ уязвимостей и защищенности системы; оценка риска, например, для случая, когда при решении задачи оценивания состояния на основе модели в форме ПС необходимо учесть корреляцию шумов поведения динамики исследуемого объекта и шумов данных наблюдений. В алгоритмах 1 и 2 при построении моделей в форме ПС, в работе [5], предполагались, что шумы динамики и шумы измерительной системы белые и гауссовские. Эти шумы между собой и начальным состоянием предполагались взаимно-некоррелированными. При этих условиях для расчетов оценок предсказаний и фильтраций использовались стандартные уравнения фильтра Калмана.

Но на практике могут встречаться случаи, когда шумы динамики и шумы измерительной системы могут быть взаимно-коррелированными. Поэтому в данной работе рассматривается алгоритм фильтра Калмана,

как вариант расширения соответствующего узла SIEM-системы, дополнительным алгоритмом для случая, когда шумы динамики и измерителей коррелированы между собой [9].

Пусть объект исследования описывается стационарными непрерывно-дискретными моделями в форме ПС вида:

$$\dot{x}(t) = A \cdot x(t) + B + C \cdot w(t),\ x(t_0) = x_0, \tag{11}$$

$$y(t_k + 1) = H \cdot x(t_k) + v(t_k), t_{k-1} \le t \le t_k, k = \overline{1, N}, \tag{12}$$

где $x - n-$вектор состояния; $\dot{x} - n-$вектор производной состояния по времени $t \ge t_0$; $w - q-$вектор шумов динамики; $y - m-$вектор наблюдений; $v - m-$вектор шумов измерителей.

Предполагается, что система представляет собой стационарный процесс. Поэтому матрицы A, B, C являются постоянными и они имеют размеры $n \times n$, $n \times r$, $n \times q$. Непрерывное время обозначается символом t, производная по времени – точкой сверху, а дискретное время через t_k. Нижний индекс отмечает порядковый номер момента времени наблюдения. Случайный процесс $\{w(t), t \ge t_0\}$ представляет собой белый гауссовский шум с нулевым математическим ожиданием и матричной корреляционной функцией вида:

$$E[w(t)w^T(\tau)] = Q \cdot \delta(t - \tau),$$

для всех $t, \tau \ge t_0$, где $\delta(t - \tau)$ – дельта функция Дирака. Матрица Q размера $q \times q$ непрерывна и неотрицательно определена для $t \ge t_0$.

Последовательность $\{v(t_k), t_k \in [t_0, t_N], k = 0, 1, 2, \ldots, N\}$ представляет собой белую гауссовскую последовательность с нулевым математическим ожиданием и матричной корреляционной функцией вида:

$$E[v(t_k) \cdot v^T(\tau_j)] = R \cdot \delta_{kj},$$

где δ_{kj} – символ Кронекера, значения которого определяются из соотношения $\delta_{kj} = \begin{cases} 1 & при \quad k = j, \\ 0 & при \quad k \ne j, \end{cases}$ для всех $t_k, \tau_j \ge t_0$. Матрица R размера $m \times m$ положительна определена для $t_k \ge t_0$. Предполагается также,

что два указанных в (11), (12) случайных процесса в дискретном представлении $w(t_k)$ и $v(t_j)$ коррелированы между собой:

$$E\left[\left(\frac{w(t_k)}{v(t_k)}\right)\cdot\left(w^T(t_k):v^T(t_k)\right)\right]=\begin{pmatrix}\tilde{Q} & S\\ S^T & R\end{pmatrix}$$

для всех $t_k \ge t_0$, при $\tilde{Q}\ge 0$, $S\ge 0$, $R>0$. Здесь S – взаимно-корреляционная матрица шумов динамики объекта и измерителя размера $q\times m$; $\tilde{Q}$ – ковариационная матрица для дискретной модели, соответствующая непрерывной модели.

При этом для оценок состояния линейной непрерывно-дискретной системы будем использовать результаты работы [9], в которой алгоритм оценивания состояния для линейных дискретных систем обобщаются на случай взаимно-коррелированных шумов объекта и измерителя.

При предположениях, указанных выше, оценки состояния будут вычисляться по следующим формулам (для непрерывной обновлённой последовательности):

$$\dot{\hat{x}}(t\,|\,t_k)=A\cdot\hat{x}(t\,|\,t_k)+B+F_0(t)\cdot\tilde{y}(t_k);\;\;\hat{x}(t_0\,|\,t_0)=x(t_0); \qquad (13)$$

$$\dot{P}(t\,|\,t_k)=A_0\cdot P(t\,|\,t_k)+P(t\,|\,t_k)\cdot A_0^{\,T}+Q_0;\;\;P(t_0\,|\,t_0)=P(t_0); \qquad (14)$$

$$K(t_{k+1})=P(t_{k+1}\,|\,t_k)\cdot H^T\cdot\left[H\cdot P(t_{k+1}\,|\,t_k)\cdot H^T+R\right]^{-1}; \qquad (15)$$

$$\hat{x}(t_{k+1}\,|\,t_{k+1})=\hat{x}(t_{k+1}\,|\,t_k)+K(t_{k+1})\cdot\left[y(t_{k+1})-H\cdot\hat{x}(t_{k+1}\,|\,t_k)\right]; \qquad (16)$$

$$P(t_{k+1}\,|\,t_{k+1})=\left[I-K(t_{k+1})\cdot H\right]\cdot P(t_{k+1}\,|\,t_k); \qquad (17)$$

где $A_0=A-F_0\cdot H$; $F_0=C\cdot S\cdot R^{-1}$; $Q_0=C\cdot Q\cdot C^T-F_0\cdot R\cdot F_0^{\,T}$, при $t_1\le t\le t_N$, $t_k\ge t_0$, $k=0,1,2,...,N$. Как видим структура алгоритмов фильтрации при взаимно-коррелированных шумах объекта и измерителя почти аналогичны алгоритму фильтрации при взаимно-некоррелированных шумах.

Существенным отличием является запись дифференциального уравнения (13) для оценок предсказания. Это уравнение содержит дополнительное слагаемое, учитывающее информацию о коррелированности шумов, и которое требует на первом этапе наблюдения знания начального состояния объекта. Этот вопрос в работе [9] остаётся открытым. Нужно заметить, что эта проблема возникает лишь в том случае, когда шумы коррелированны. Здесь, видимо, можно предложить два способа оценки наблюдения для состояния в момент запуска объекта. Первый способ состоит в том, что мы для достаточно малых временных интервалов проводим серию наблюдений и, предполагая, что шумы некоррелированны и используя алгоритм фильтрации при некоррелированных шумах определяем серию оценок предсказания наблюдений. Затем производим по этим известным оценкам наблюдений предсказания на один шаг назад. На практике можно столкнуться со случаями, когда связь между шумами объекта и измерителя тесная. Тогда вышеизложенный способ может привести к плохой оценке наблюдения для начального состояния объекта. В этом случае, видимо, проще использовать уравнения наблюдения для оценки в момент запуска системы.

Информация о взаимной корреляции шумов динамики и измерительной системы содержится также в уравнении (14), тогда как уравнение расчета корреляционной матрицы ошибки оценок предсказания в стандартных уравнениях фильтра Калмана такого слагаемого не содержит.

Заметим, что на практике могут возникать различные случаи описания поведения объекта, например: случай, когда данные выхода измерительной системы коррелированы между собой; описание поведения исследуемого объекта в виде нелинейных соотношений в моделях в форме ПС [8]; описание поведения объекта в виде нестационарных моделей в форме ПС [17, 18] и т. д. Все эти случаи должны быть реализованы различной совокупностью уравнений в алгоритмах 1 и 2 при выполнении расчетов относительно оценок предсказания и фильтрации в соответствующих узлах SIEM системы.

5. ОЦЕНИВАНИЕ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ И ОПТИМАЛЬНЫЙ ВЫБОР СРЕДСТВ ДЛЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ

Состояние защищенности ИР предприятия не является постоянным и находится в прямой зависимости от уровня технического, программного, экономического развития, прибыли (дохода), стоимости материальных ценностей предприятия. При этом существуют следующие связи [19]:

– увеличение объема прибыли, материальных ценностей влечет необходимость повышения уровня защищенности ИР;

– с увеличением величины прибыли возрастает число угроз ИБ;

– увеличение числа угроз и появление новых уязвимостей вызывает необходимость улучшения качества защиты информации на предприятии;

– для повышения уровня защищенности ИР и информации увеличивают затраты на ее защиту;

– увеличение уровня защиты информации предприятия снижает уровень воздействия угроз.

Таким образом, состояние защищенности ИР в ИС предприятия находится в объективной связи как с уровнем технического, программного, экономического развития, так и с возможностями угроз по нанесению ему материального ущерба.

Если относиться к вложениям в ИБ как к затратам, то сокращение этих затрат позволит решить тактическую задачу освобождения средств. Однако, это заметно отдалит компанию от решения стратегической задачи. Поэтому, если у компании есть долгосрочная стратегия

развития, она рассматривает вложения в ИБ как инвестиции. Именно такой подход позволяет определить цели и задачи построения комплексной, активной системы защиты информации [20] с элементами интеллектуальных сервисов [1–3], предусмотренных в SIEM-системах.

5.2. ОПТИМАЛЬНЫЙ ВЫБОР СРЕДСТВ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВОЗМОЖНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалисты в области ИБ предлагают различные методы оценки эффективности инвестиций в систему ИБ. Например, в [19] автор описывает подход к оценке эффективности управления рисками, который подразумевает под собой вложение инвестиций. Для построения экономически эффективной системы защиты необходимо решить задачу оптимального выбора средств реализации системы защиты ИР от комплекса возможных угроз информации [20]. Такие задачи необходимо решать, опираясь на существующие математические методы. Например, для выбора средства эффективной защиты от различного рода атак можно использовать методы теории игр [6, 21].

Теория игр предполагает наличие продавца и покупателя. Матричная игра, в которой игрок взаимодействует с окружающей средой, решает задачу определения наиболее выгодного варианта поведения с учётом неопределённости состояния окружающей среды и которая называется статистической игрой. Игрок в таком случае называется лицом, принимающим решение (ЛПР) [21].

5.2.1. ПОСТАНОВКА ЗАДАЧИ

Взаимосвязь между продавцом и покупателем определяется платежной матрицей. В общем виде платёжная матрица статистической игры состоит из: строк A_i – стратегии ЛПР; столбцов матрицы S_j – состояния окружающей среды; $\{ w_{ij}, i = \overline{1,m}, j = \overline{1,n} \}$ – ожидаемый выигрыш при использовании стратегии A_i в случае, если среда находится в состоянии S_j.

В практике принятия решений, ЛПР руководствуется следующими возможными критериями принятия решений: критерием Вальда, критерием Гурвица, критерием Сэвиджа и др. [21].

В нашем случае, когда необходимо выбрать средство защиты информации в зависимости от различных типов атак, будем осуществлять выбор согласно критерию Вальда.

Критерий Вальда обеспечивает выбор осторожной пессимистической стратегии в той или иной деятельности: для каждого решения выбирается самая худшая ситуация (наименьшее из w_{ij}) и среди них отыскивается гарантированный максимальный эффект

$$W = \max_j \min_i w_{ij}\,,\ i = \overline{1,m}\,,\ j = \overline{1,n}.$$

Можно принять и критерий выбора оптимистической стратегии

$$W = \min_i \max_j w_{ij}\,,\ i = \overline{1,m}\,,\ j = \overline{1,n}\,,$$

где оценивается гарантированный выигрыш при самых благоприятных условиях.

В критерии Гурвица происходит ориентация на самый худший исход, что является своеобразной подстраховкой. Однако, опрометчиво выбирать политику, которая излишне оптимистична. Критерий Гурвица предлагает некоторый компромисс:

$$W = \max\left[\alpha \max W_{ij} + (1-\alpha)\min W_{ij}\right],\ i = \overline{1,m}\,,\ j = \overline{1,n}\,, \qquad (18)$$

где параметр α принимает значение от 0 до 1 и выступает как коэффициент оптимизма.

Допустим, известны следующие показатели: A_{ir_i} – группы атак; m – количество групп атак $\{i = \overline{1,m}\}$; r_i – количество атак в группе i; $\left\{S_j\,,\ j = \overline{1,n}\right\}$ – средства защиты; n – количество средств защиты; X_1, $X_2,\ldots,X_n$ – стоимость применяемого средства защиты; Y – величина предполагаемого ущерба; w_{ir_ij} или $\{\left\{p^{(3)}_{ir_ij}; i = \overline{1,m},\ j = \overline{1,n}\right\}$ – вероятность защиты, т. е. вероятность отражения атаки A_{ir_i} при использовании средства защиты S_j; $p^{(a)}_{ir_i}$ – вероятность проведения атаки;

$p_{ir_i j}^{(y)}$ – вероятность нанесения ущерба при i-ой атаке и j-м средстве защиты с учетом частоты использования i-ой атаки.

В соответствии с видом платежной матрицы представим вероятности отражения атаки в следующей табл. 8:

Таблица 8

Вероятности отражения атаки

Группы атак		Средства защиты			
		S_1	S_2	…	S_n
		Вероятности отражения атаки			
	A_{11}	$p_{111}^{(3)}$	$p_{112}^{(3)}$	…	$p_{11n}^{(3)}$
	…	…	…	…	…
	A_{1r1}	$p_{1r11}^{(3)}$	$p_{1r12}^{(3)}$	…	$p_{1r1n}^{(3)}$
	…	…	…	…	…
	A_{mr_m}	$p_{mr_m1}^{(3)}$	$p_{mr_m2}^{(3)}$	…	$p_{mr_mn}^{(3)}$

Как правило, ни одно из средств защиты не обеспечивает защиту ИР на 100 %, поэтому вероятности отражения атак будут строго меньше 1.

Далее в табл. 9 представлена стоимость средств защиты.

Таблица 9

Стоимость средств защиты X_j, j = 1, 2, 3, … n

Средства защиты	S_1	S_2	…	S_n
Стоимость средств защиты	X_1	X_2	…	X_n

Необходимо отметить, что неограниченное вложение денежных средств не означает гарантированную защиту ИР.

Условием эффективной защиты является следующее правило: стоимость средств защиты должна быть меньше стоимости потерь, понесенных при успешной реализации атаки. Все статистические данные могут быть взяты из отдела ИБ предприятия или репозитория в соответствующих узлах SIEM-систем.

5.2.2. МЕТОДИКА РЕШЕНИЯ ЗАДАЧИ

Утверждение

Критерий «стоимость–эффективность»: общая стоимость средств защиты должна быть меньше стоимости потерь, понесенных при успешной реализации атак. Математическое выражение критерия «стоимость-эффективность» будет соответствовать неравенству:

$$\lambda_{ir_i j} = \frac{X_j}{\left(1 - p^{(3)}_{lr_i j}\right) \times p^{(a)}_{ir_i} \times Y} \le 1 ;\ i = \overline{1,m} ,\ j = \overline{1,n} . \qquad (19)$$

Доказательство

Вероятность того, что мы применим одно из средств защиты равна 1 (100 %). Составим следующее неравенство:

$$1 \times X_j \le p^{(y)}_{ir_i j} \times Y ;\ i = \overline{1,m} ,\ j = \overline{1,n} . \qquad (20)$$

Представим вероятность нанесения ущерба $p^{(y)}_{lr_i j}$ через вероятность защиты от атаки $\left(p^{(3)}_{lr_i j}\right)$ и вероятность проведения атаки $\left(p^{(a)}_{lr_i}\right)$:

$$p^{(y)}_{ir_i j} = \left(1 - p^{(3)}_{lr_i j}\right) \times p^{(a)}_{ir_i} ;\ i = \overline{1,m} ,\ j = \overline{1,n} . \qquad (21)$$

Подставив (21) в (20), получим:

$$X_j \le \left(1 - p^{(3)}_{lr_i j}\right) \times p^{(a)}_{ir_i} \times Y ;\ i = \overline{1,m} ,\ j = \overline{1,n} . \qquad (22)$$

Разделив обе части соотношения (22) на выражение, стоящее в правой части этого неравенства, получим:

$$\frac{X_j}{\left(1 - p^{(3)}_{lr_i j}\right) \times p^{(a)}_{ir_i} \times Y} \le 1 ;\ i = \overline{1,m} ,\ j = \overline{1,n} . \qquad (23)$$

Обозначим в (23) левую часть неравенства через λ_{ir_ij} и назовем коэффициентом эффективной защиты:

$$\lambda_{ir_ij} = \frac{X_j}{\left(1 - p^{(3)}_{lr_ij}\right) \times p^{(a)}_{ir_i} \times Y}; \; i = \overline{1,m}, \; j = \overline{1,n}.$$

Учитывая нестрогое неравенство (23) приходим к выводу, что математическим выражением условия эффективной защиты будет соотношение:

$$\lambda_{ir_ij} \le 1; \; i = \overline{1,m}, \; j = \overline{1,n} \qquad (24)$$

что и требовалось доказать. Коэффициенты эффективной защиты представлены в табл. 10.

Таблица 10

Матрица коэффициентов эффективной защиты при величине предполагаемого ущерба *Y* с выбором средства эффективной защиты

Атаки	Вероятность использования злоумышленником различных групп атак	Средства защиты			
		S_1	S_2	…	S_n
		Коэффициенты эффективной защиты			
A_{11}	$p^{(a)}_{11}$	λ_{111}	λ_{112}	…	λ_{11n}
…	…	…	…	…	…
A_{1r_1}	$p^{(a)}_{1r_1}$	λ_{1r_11}	λ_{1r_12}	…	λ_{1r_1n}
A_{21}	$p^{(a)}_{21}$	λ_{211}	λ_{212}	…	λ_{21n}
…	…	…	…	…	…
A_{mr_m}	$p^{(a)}_{mr_m}$	λ_{mr_m1}	λ_{mr_m2}	…	λ_{mr_mn}

Условие (24) будем использовать наряду с критерием Вальда. Правило выбора решения в соответствии с максиминным критерием Вальда можно интерпретировать следующим образом. Платёжная матрица (табл. 10) дополняется строкой, каждый элемент которой представляет собой минимальное значение выигрыша в соответствующей стратегии ЛПР (при этом пусть $k = r_1 + r_2 + \cdots + r_m + 1$):

$$W_{kj} = \min w_{ij}, \; i = \overline{1,m}, \; j = \overline{1,n}.$$

Оптимальной по данному критерию считается та стратегия ЛПР, при выборе которой минимальное значение выигрыша максимально:

$$W = \max W_{kj}\,,\ k = r_1 + r_2 + \cdots + r_m + 1\,,\ j = \overline{1,n}\,.$$

Выбранная, таким образом, стратегия полностью исключает риск. Это означает, что принимающий решение не может столкнуться с худшим результатом, чем тот, на который он ориентируется.

Предложенная выше методика эффективного выбора средств защиты ИР в КС позволяет в режиме реального времени выдавать рекомендации в соответствующих узлах SIEM-систем не только эффективного выбора средств защиты, но и учитывать весь объем финансирования как ограничения на приобретения этих средств защиты.

6. ЗАКЛЮЧЕНИЕ

Выше представлены следующие положения:

– приведены требования к современным СУИБ и принципы их построения;

– систематизировано изложены математические методы и модели в форме пространства состояний для последующего анализа контролей безопасностей, которые были нацелены на изучение объективных подходов для защиты ИР в КС;

– сформулированы и показаны практического характера шаги расчета объективных оценок зависящих от использования различных типов структур моделей в форме ПС и различных взаимоотношений и свойств составляющих компонентов используемых при описании количественных характеристик показателей поведения исследуемых объектов, которые учитывались экспертами для предложения своих экспертных оценок для расчета рисков относительно исследуемых информационных систем.

Для обеспечения непрерывного функционирования современного бизнеса необходима устойчиво функционирующая СУИБ, базирующаяся на процессе «Управление информационной безопасностью». Результативность СУИБ обеспечивается уровнем зрелости процессов информационной безопасности и основных процессов информационных технологий. Правильно выстроенный и функционирующий процесс «Управление информационной безопасностью» повышает зрелость ИТ организации до третьего уровня модели СММ (уровень управляемости). Основнополагающим процессом, позволяющим СУИБ быть актуальной, является процесс «Управление рисками», являющийся частью стратегического бизнес-процесса «Управление информационной безопасностью».

Управление рисками основано, прежде всего, на объективных статистических данных, которые: фиксируются, накапливаются, анализируются, хранятся, обрабатываются для целей оценивания потенциального ущерба от ошибок пользователей и атак нарушителей на ИР в ИС

предприятия на основе данных, хранящихся в репозитории SIEM-систем, а также выбора средств защиты ИР для минимизации ущерба, расчета оценок предсказания и фильтрации всех возможных параметров и показателей, связанных с ИБ. В частности, были предложены методики, позволяющие рассчитывать оценки объективной вероятности в возможности наступления различных видов НС, оценки объективной стоимости ущерба от нарушений безопасности ИР в ИС предприятия и оценки предсказания и фильтрации величины ущерба. Все основные расчеты показателей ИБ в ИС предприятия нацелены на использовании возможностей стохастических моделей в форме ПС и уравнений фильтра Калмана для получения более достоверных значений оценок фильтрации состояния исследуемого объекта.

Предложена методика эффективного выбора средств защиты ИР в КС – как рекомендация поставляемая соответствующими узлами SIEM-систем, которая учитывает весь объем финансирования выделяемого предприятием для защиты ИР ИС как ограничение на приобретение средств защиты.

ЛИТЕРАТУРА

1. *Котенко И.В.*, *Саенко И.Б.* SIEM-системы для управления информацией и событиями безопасности. – М,: INSID,2012. – № 5. – 54– 65 с.

2. *Miller D. R.*, *Harris Sh.*, *Harper A.A. Van-Dyke S.*, *Black Ch.* Security Information and Event Management (SIEM) Implementation: McGrawHill Companies, 2011. – 430 p.

3. *Muhammad Afzaal*, *Cesario Di Sarno*, *Salvatore D'Antonio*, *Luigi Romano*. An Intrusion and Fault Tolerant Forensic Storage for SIEM System: Eighth International Conference on Signal Image Technology and Internet Based System, 2012. – 579–586 p.

4. *Cross Mark*, *Saso Karakatic*, *Vili Podgoreles*. Improved classification with allocation method and multiple classifiers: Information Fusio, 2016. 31. – 26–42 p.

5. *Абденов А.Ж.*, *Заркумова-Райхель Р.Н.* Оценивание риска в информационных системах на основе объективных и экспертных оценок: вопросы защиты информации, 2015, № 1. – 64–70с.

6. *Абденов А.Ж.*, *Заркумова Р.Н.* Выбор средства эффективной защиты с помощью методов теории игр: вопросы защиты информации, 2010. – № 2. – 26–31с.

7. *Абденов А.Ж.*, *Трушин В.А.*, *Абденова Г.А.*, *Иноземцева Ю.А.* Методика расчета рисков на основе объективных и субъективных оценок в соответствующих узлах SIEM-системы: Искусственный интеллект и принятие решений. – 2016. – № 3. – 87–99 с.

8. *Novikova E.*, *Kotenko I.* Analytical Visualization Techniques for Security Information and Event Management: 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing. 2013. – 519–525 с.

9. *Синицын И.Н.* Фильтры Калмана и Пугачева: учебное пособие – М.: Университетская книга, Логос, 2006. – 640 с.

10. *Симкин М.М.* О рекуррентной фильтрации при взаимно-коррелированных шумах объекта и измерителя: Автоматика и телемеханика. – 1980. – № 1. – 71–80 с.

11. *Luigi Coppolino*, *Salvatore D'Antonio*, *Valerio Formicola*, *Luigi Romano*. A framework for mastering heterogeneity in multi-layer security information and event correlation: Journal of Systems Architecture. – 2015. – 1–15 p.

12. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. 2008. – 56 p.

13. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. ENISA (European Network and Information Security Agency). – 2006. – 168 p.

14. *Chi-Chun Lo*, *Wan-Jia Chen*. A hybrid information security risk assessment procedure considering interdependences between controls: Expert Systems with Applications. – 2011. – V. 39. – 248–257p.

15. *Vose D*. Risk Analysis: F Quantitative guide, 3-rd edition. John Wiley & Sons, 2008. – 752 p.

16. *Kumamoto H*., *Henley E*. Probabilistic risk assessment and management for engineers and scientists.2-nd edition.Institute of Electrical and Electronics Engineers. Inc. New York, 1996. – 620 p.

17. Информационная безопасность. Уровни зрелости СУИБ организации. Доступ в Интернете: http://www.wikisec.ru..

18. NIST SP 800-30:2012. Guide for conducting Risk Assessments [электронный ресурс] // National Institute of Standards and Technology. – URL: http:// csrc.nist.gov/publications/PubsSPs.html (Дата обращения: 29.05.2013); – 22р.

19. *Гайшун И.В*. Идентификация линейных нестационарных систем по реакции на обобщенные управления: Дифференц. уравнения. 2008. 44. – 301–307 с.

20. *Богословский С.В*., *Богословский В.С*. Динамика нестационарных систем с равномерно изменяющимися во времени коэффициентами: науч. приборостр. 2002. 12. – № 3. – 83–92 с.

21. *Баранов Д*. Оценка эффективности управления рисками: Информационная безопасность, Information Security, 2004. – № 2. – 26–27 с.

22. *Теренин А.А*. Проектирование экономически эффективной системы информационной безопасности: Защита информации, INSIDE, 2005. – № 1. – 26–35 с.

23. *Оуэн Г*. Теория игр. – М.: Мир, 1971. – 230 с.

24. ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».

25. ISO/IEC 27002 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».

26. СТО БР ИББС – комплект документов Стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

27. NIST SP 800 – набор стандартов по ИБ National Institute of Standards and Technology.

28. ITIL – библиотека, описывающая лучшие из применяемых на практике способов организации работы подразделений или компаний, занимающихся предоставлением услуг в области информационных технологий.

29. CobiT – пакет открытых документов, около 40 международных и национальных стандартов и руководств в области управления IT, аудита и IT-безопасности.

30. ITSM (IT Service Management, управление ИТ-услугами) – документы, описывающие подход к управлению и организации ИТ-услуг, направленный на удовлетворение потребностей бизнеса.

ПРИЛОЖЕНИЕ 1

Термины и определения

Актив	–	все, что имеет ценность для организации и находится в ее распоряжении
ИБ	–	информационная безопасность
Информация	–	сведения (сообщения, данные) независимо от формы их представления
Инфраструктура	–	комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи)
Информационная инфраструктура	–	система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия
ИТ	–	информационные технологии
ИС	–	информационные системы
SIEM	–	Security Information and Event Management (управление информацией и событиями безопасности)
СИБ	–	система информационной безопасности
СУИБ	–	система обеспечения информационной безопасности
СУИБ	–	система управления информационной безопасностью
КИ	–	конфиденциальная информация
ИР	–	информационные ресурсы
КС	–	компьютерная система
MASSIF	–	MAnagement of Security Information and Event in Service Infrastructure (Управление информацией и событиями безопасности в инфраструктурах услуг)
logs	–	записи в различных журналах аудита
СППР	–	система поддержки принятия решений
НС	–	неблагоприятное событие
Репозиторий	–	хранилище – место, где хранятся и поддерживаются какие-либо данные. Чаще всего данные в **репозитории** хранятся в виде файлов.
SOAP	–	от англ. *Simple Object Access Protocol* – простой протокол доступа к объектам
SOA	–	англ. *service-oriented architecture* (сервис-ориентированной архитектуры)
СУБД	–	система управления базами данных

ОГЛАВЛЕНИЕ

Абденов Амирза Жакенович
Дронова Галина Александровна
Трушин Виктор Александрович

СОВРЕМЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебное пособие

В авторской редакции

Выпускающий редактор *И.П. Брованова*
Дизайн обложки *А.В. Ладыжская*
Компьютерная верстка *Л.А. Веселовская*

Налоговая льгота – Общероссийский классификатор продукции
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

Подписано в печать 25.05.2017. Формат 60 × 84 1/16. Бумага офсетная. Тираж 50 экз.
Уч.-изд. л. 2,79. Печ. л. 3,0. Изд. № 153. Заказ № 756. Цена договорная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20