УДК 621.391

АНАЛИЗ ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ БАНКОВСКОЙ ИНФОРМАЦИИ

Евсеев С.П., Сочнева А. С., Король О.Г.

Анализируется понятие банковской информации, основные источники угроз банковской информации, рассматриваются методы аномалий и злоупотреблений, модели и методики оценки рисков кибербезопасности.

Ключевые слова: методы аномалий и злоупотреблений, безопасность информации, кибернетическая безопасность, угрозы банковских данных.

1. Введение

Важное значение в обеспечении безопасности государства, и особенно экономической ее составляющей, является защита ее рыночных основ, определяющих экономическую составляющую конкуренции. Развитие государства тесно связано с развитием рыночных отношений и рентабельной конкурентоспособной экономики, в которой банковский сектор играет главную роль. Революционные изменения последнего десятилетия в электронной индустрии, объединение инфокоммуникационных и компьютерных сетей в единое пространство существенно расширили спектр услуг автоматизированных банковских систем (АБС), при этом одной из наибольшей небезопасной угрозой для экономики государства является нарушение ее финансово-банковской системы. Таким образом, решение вопросов обеспечения безопасности транзакций в АБС остается актуальной и на сегодняшний день.

2. Анализ литературных данных и постановка проблемы

Компьютерные системы и телекоммуникации обеспечивают надежность функционирования огромного количества информационных систем самого разного назначения. Большинство таких систем несут в себе информацию, имеющую конфиденциальный характер. Таким образом, решение задачи автоматизации процессов обработки данных повлекло за собой новую проблему – проблему информационной безопасности [1]. Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связана с использованием автоматизированных систем обработки информации банка (АСОИБ) [2]. Защита собственно банковской системы должна использовать мощные средства аутентификации и контроля действий как внутренних пользователей, так и клиентов. Общепринято, что наиболее

надежную защиту могут обеспечить средства двухфакторной аутентификации, будь то электронные ключи (токены) или генераторы одноразовых паролей. Безопасность данных при хранении требует использования средств шифрования, которые смогут работать либо на уровне хранилищ данных, либо на уровне отдельных компонентов системы, например, таблиц баз данных. Безопасность банкоматов и платежных терминалов должна обеспечиваться с использованием традиционных средств – антивирусной защиты. Но в то же время специфика таких устройств требует применения дополнительных средств защиты, включая создание “замкнутой программно-аппаратной среды”, полностью исключающей установку любого стороннего ПО и подключение внешних устройств [3]. Для обеспечения адекватности системы защиты информации целесообразно применять принципы Риск-менеджмента. Данный метод позволит, при грамотном подходе определить и классифицировать угрозы и, в соответствии с вероятностью наступления негативных последствий и их возможной тяжестью для Банка, организовывать Систему защиты. К сожалению, на сегодня принципы Риск-менеджмента в сфере защиты информации еще не очень совершенны [4]. На практике обеспечение информационной безопасности происходит в условиях случайного воздействия факторов, которые в полной мере сложно предусмотреть заранее при проектировании системы защиты информации, но в дальнейшем они способны снизить эффективность предусмотренных проектом мер информационной безопасности или полностью скомпрометировать их.

Одной из существенных проблем при проектировании и эксплуатации систем защиты информации является игнорирование методологии системного анализа в отношении средств и инструментов для их защиты. Следует признать сложность, а иногда и невозможность объективного подтверждения эффективности системы защиты информации, что во многом определяется неполнотой нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев [5]. Международный стандарт для операций по банковским картам с чипом (EMV), введенный в 2005 году, определяет физическое, электронное и информационное взаимодействие между банковской картой и платёжным терминалом для финансовых операций на основе стандартов ISO/IEC 7816 для контактных карт, и ISO/IEC 14443 для бесконтактных карт. Интернет-банкинг широко распространился среди банков и клиентов. Использование Интернет-ресурсов в качестве альтернативного средства передачи пин-кода клиента в банк не только приводит к снижению затрат на передачу, но и позволяет улучшить банковскую конкурентоспособность и увеличить гибкость работы банка с клиентами. Главными препятствиями на пути интернет-банкинга являются безопасность системы, отсутствие доверия и правовой поддержки [6]. В работе [7] отмечается, что безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

3. Цели и задачи исследования

Целью работы является анализ понятия банковской информации, основные источники угроз банковской информации, рассматриваются методы аномалий и злоупотреблений, моделей и методик оценки рисков кибербезопасности в автоматизированных банковских системах.

4. Анализ структуры банковской информации.

Учитывая стремительное развитие науки и техники за последние десять лет, а также интенсивное применение новейших высокотехнологических разработок в банковском секторе сущность и содержание категории “банковская информация” существенно изменилась. Сегодня, как известно, банковская информация является основой компонентой современных АБС. Исходя из этого и опираясь на [8, 14] можно утверждать, что под банковской информацией в самом широком смысле понимается совокупность сведений, связанных с Уставными документами и Руководством банковского учреждения, организационно-правовой формой банковской учреждения, нынешним видом банковского учреждения и ее служащих, видами и формами банковского обслуживания, количеством и составом клиентов, операциями по счетам клиентов, наличием корреспондентских отношений и техническим обеспечением банка. Учитывая широту объятия категории банковская информация с целью дальнейшего ее корректного применения предлагается признаковая классификация банковской информации (рис. 1).

Рис. 1. Признаковая классификация банковской информации

Преимуществом предложенной признаковой классификации банковской информации (см. рис. 1) является то, что она в отличие от известных классификаций позволяет раскрыть глубину содержания сущности данной категории. Например, по видам банковская информация бывает организационной, технологической и параметрической. При этом под *организационной банковской информацией* следует понимать информацию отображающую характер деловых связей банка с клиентами, информацию про

особенности организации и построения системы управления банка. *Технологическая банковская информация* – это информация о принципах управления банком при осуществлении им всех видов банковской деятельности, а также информация о применяемых в системах банковской защиты новейших высокотехнологических разработок. *Параметрическая банковская информация* – это информация отражающая количественные показатели, отображающие банковский капитал и величину его кредитного портфеля при осуществлении банком всех видов деятельности. Еще одним преимуществом предложенной классификации является то, что в случае появления новых признаков, характеризующих те или иные аспекты категории банковская информация в предложенной классификации предусмотрена возможность расширения множества признаков.

Из предложенной классификации также следует вывод о том то, что в подсистемах АБС Банка циркулирует информация различных уровней конфиденциальности (секретности) от открытой информации, до сведений, содержащих информацию с ограниченным доступом (коммерческая, банковская и служебная тайна). В документообороте АБС Банка также присутствуют: платежные поручения и другие расчетно-денежные документы, отчеты (финансовые, аналитические и др.), сведения о лицевых счетах, обобщенная информация и другие конфиденциальные (ограниченного распространения) документы и т.д., которые также могут быть отнесены к понятию банковской информации.

Таким образом, в самом общем виде под *банковской информацией* можно понимать информацию, которая возникает в результате банковской деятельности. Это прежде всего сведения, характеризующие сам банк, его финансовое положение, надёжность и выполнение требований законодательства. Такую информацию можно почерпнуть из устава банка, его лицензий, бухгалтерских балансов, отчетов о прибыли и убытках и других источников. Кроме того, в более узком понимании банковская информация – это сведения о конкретных операциях банка. Такая информация характеризует не только банк, но и тех лиц, с которыми банк вступает в правоотношения. В качестве примера банковской информации можно привести сведения о наличии счетов или вкладов и об операциях по ним, об имуществе, находящемся на хранении в банке.

5. Анализ основных источников угроз безопасности данных в АБС

Для анализа основных видов угроз безопасности банковской информации используем известную модель безопасности – триады CIA (confidentiality, integrity, availability) в трех сферах (профилях) безопасности: информационной безопасности, безопасности информации и кибернетической безопасности.

В данной модели под *информационной безопасностью* понимается процесс обеспечения конфиденциальности, целостности и доступности информации клиентами/клиентом банка на основе совокупности коллективного и индивидуального сознания. В рассматриваемой модели под *конфиденциальность*ю понимается обеспечение доступа к информации только авторизованным пользователям, под *целостностью* – обеспечение

достоверности и полноты информации, и методов ее обработки для авторизованных пользователей, под *доступностью* – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Безопасность информации – состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность. *Безопасность информации* определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Кибербезопасность – набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз. Кибербезопасность охватывает такие понятия, как защита персональной информации, а именно обнаружение, избежание или реакция на атаки. Стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity – дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур (см. рис. 2).

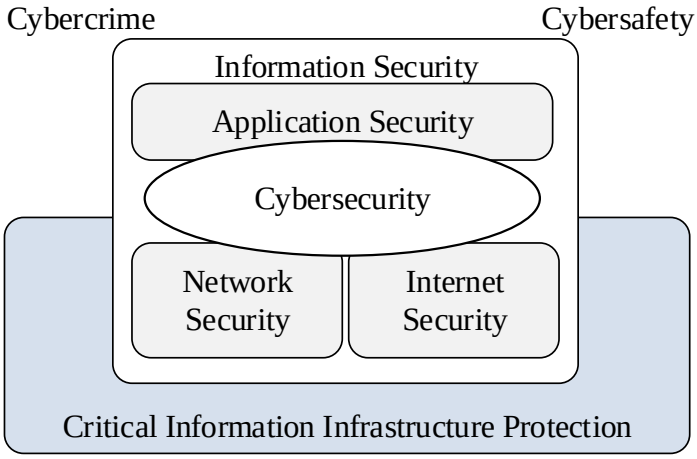

Рис. 2. Взаимосвязь между кибербезопасностью и другими доменами безопасности

Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты АБС подвержена различным угрозам, общая классификация угроз приведена в трех сферах безопасности на рис. 3.

Угрозы банка – потенциально возможные или реальные действия злоумышленников или конкурентов, способные нанести банку материального или морального вреда [9].

По происхождению источников угрозы: внутренние и внешние. Как первые, так и вторые по направленности и характеру воздействия на деятельность банков могут быть экономическими, физическими и интеллектуальными.

Экономические угрозы: коррупция, мошенничество, недобросовестная конкуренция, использование банками неэффективных технологий банковского производства. Реализация таких угроз ведет к причинению убытков банкам или упущения ними выгоды.

Физические угрозы: кражи, грабежи имущества и средств банков, поломки, вывод из строя оборудования банков, неэффективна его эксплуатация. В результате реализации таких угроз наносятся убытки банкам, связанные с потерей своей собственности и необходимостью нести дополнительные расходы на восстановление средств производства и других материальных средств.

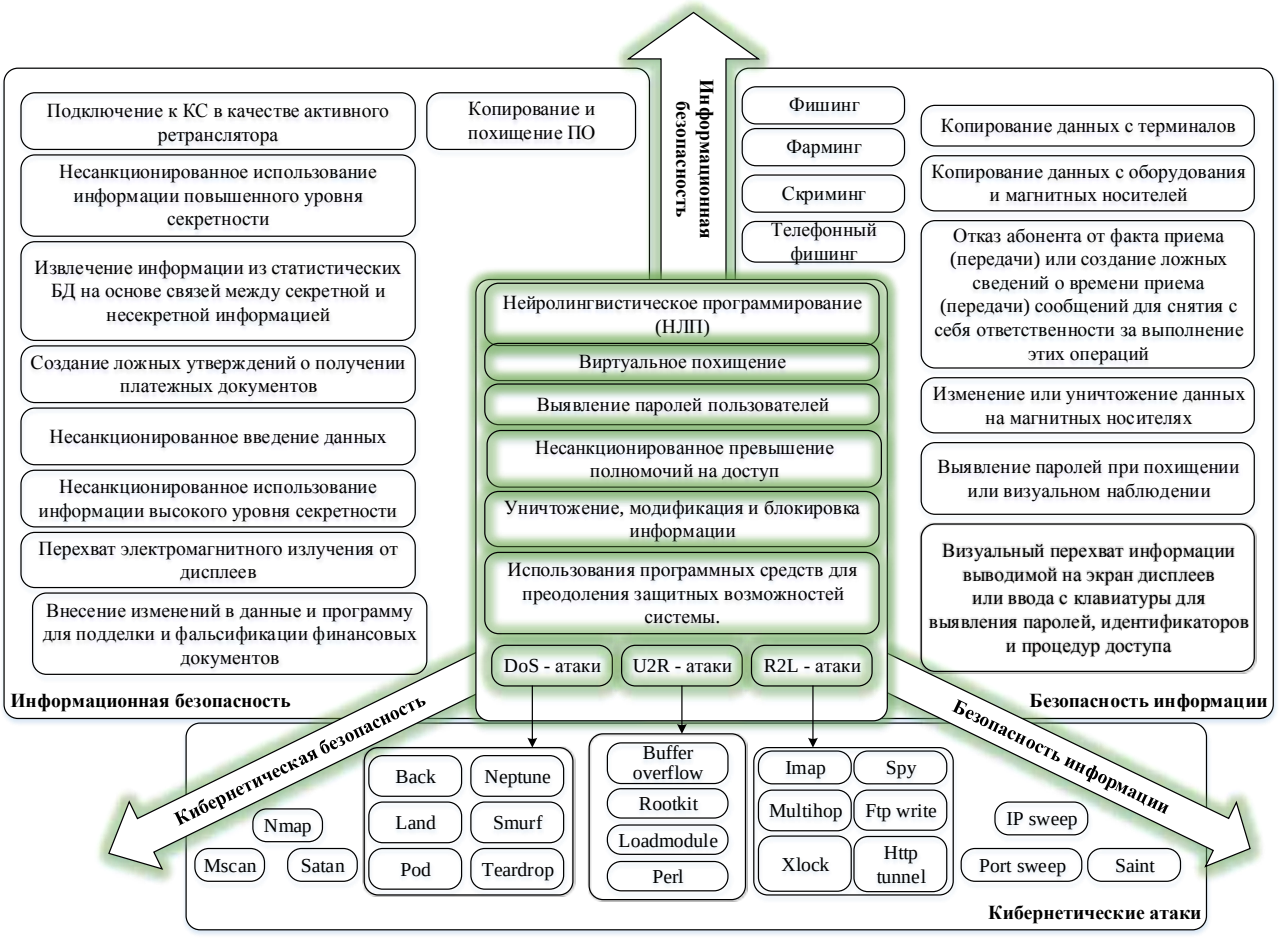

Рис. 3. Общая классификация угроз АБС

Интеллектуальные угрозы: разглашение или неправомерное использование банковской информации, дискредитация банка на рынке банковских услуг, разного рода социальные конфликты вокруг банковских учреждений или в них самих. Последствия реализации таких угроз: убытки банков, ухудшение их имиджа, социальная или психологическая

напряженность вокруг учреждения банков или в их коллективах.

Проведенный анализ показал, что одним из наиболее уязвимых мест в комплексной АБС является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом, связанная со следующими особенностями:

– внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

– взаимодействие отправителя и получателя электронного документа осуществляется опосредовано через канал связи.

Эти особенности порождают следующие проблемы:

– взаимное опознавание абонентов (проблема установления взаимной подлинности при установлении соединения);

– защита электронных документов, передаваемых по каналам связи (проблемы обеспечения конфиденциальности и целостности документов);

– защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

– обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости) [3].

Результаты исследований компании “Arbor Networks” (июнь 2015 г.) атак на компьютерные сети приведены на рис. 4.

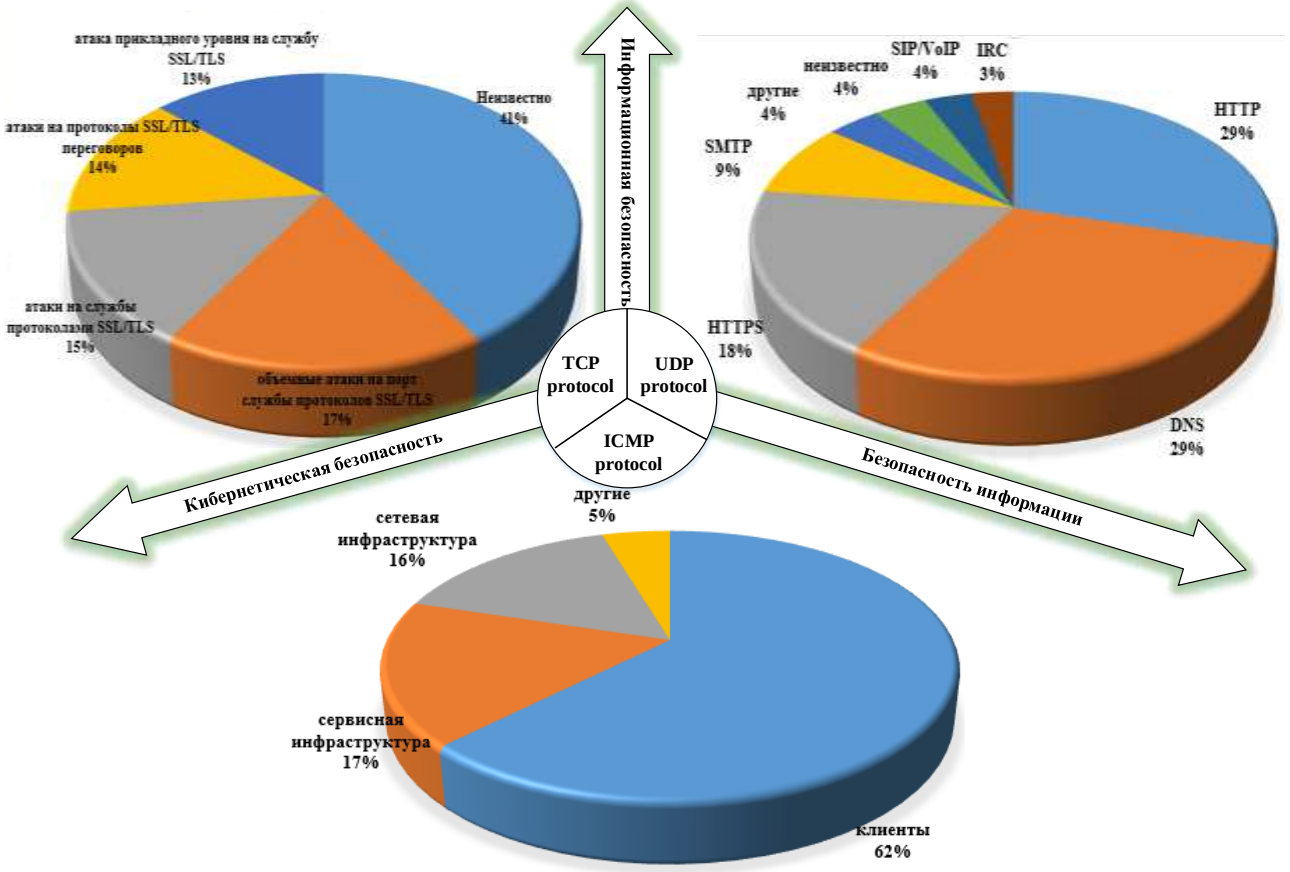

Рис. 4. Исследование угроз на протоколы IP-сетей

Проведенный анализ рис. 4 показал, что с ростом киберпреступности и вычислительных возможностей злоумышленников наблюдается дальнейшее совершенствование известных кибератак и появление новых.

Основная классификация кибератак представлена на рис. 5.

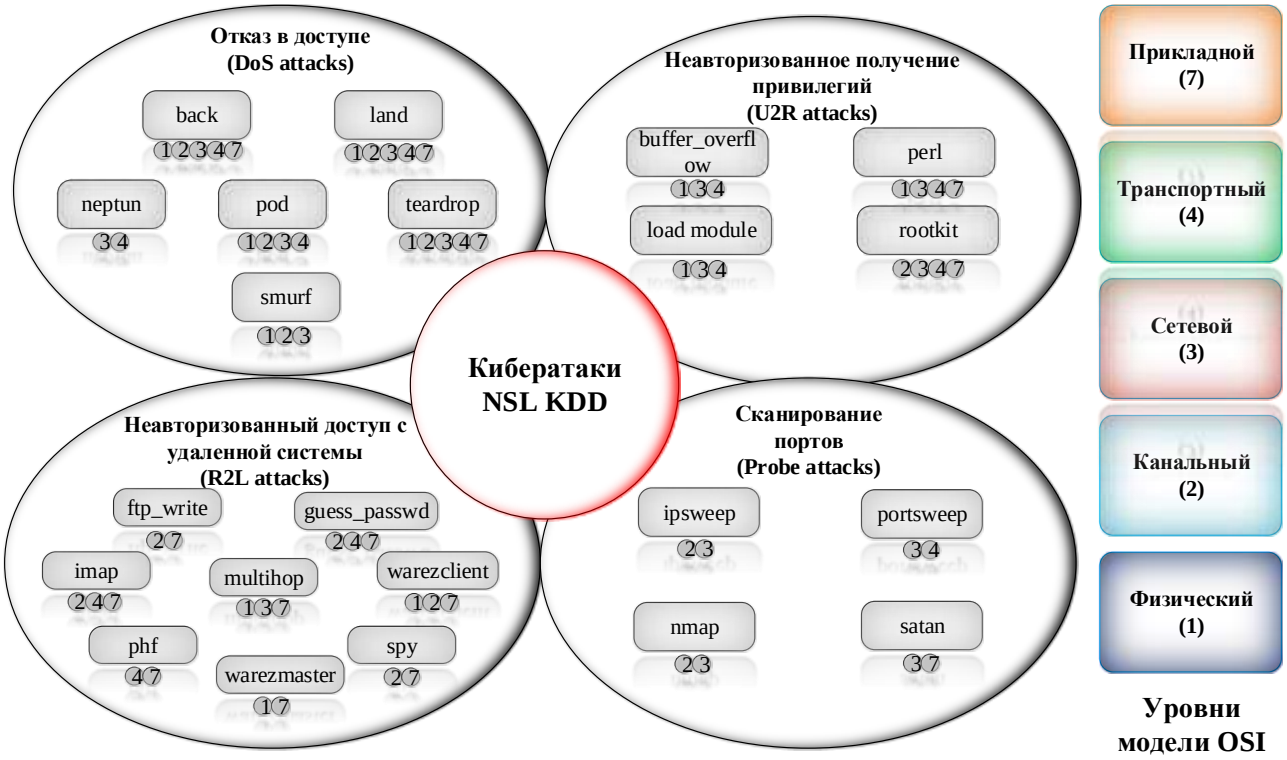

Рис. 5. Классификация кибератак

На рис. 6 приведены результаты мониторинга кибератак в указанный период на АС прокуратуры г. Киева.

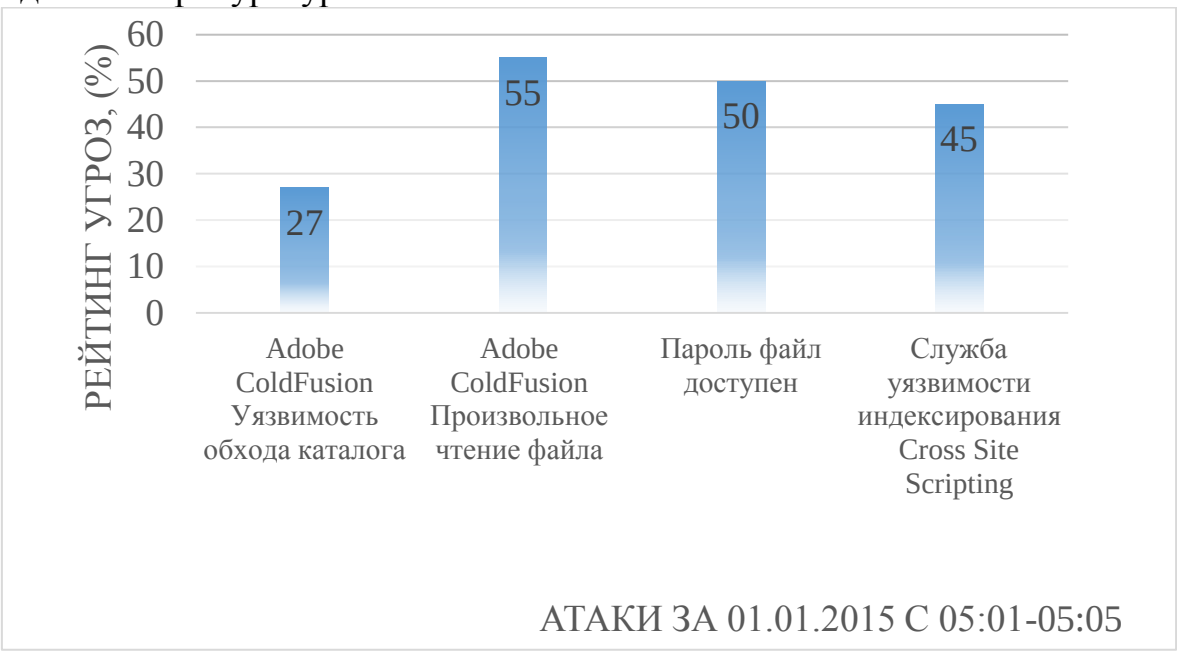

Рис. 6. Результаты мониторинга кибератак СВА

Проведенный анализ рис. 3 – 6 подтверждает пропорциональный рост кибератак с эволюционным ростом вычислительной техники в последние десятилетия и компьютерной грамотностью злоумышленников.

Основой управления информационной безопасностью АБС является анализ рисков. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам.

3. Анализ *методов аномалий и злоупотреблений, модели и методики оценки рисков кибербезопасности.*

Обычно выделяют две основные группы методик расчёта рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. Вторая группа методик оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

Для выявления аномалий (отклонений) от нормальной работы АБС используются методы выявления аномалий, общая классификация и основные характеристики представлены в табл. 1.

Таблица 1

Методы обнаружения аномалий и злоупотреблений

Метод	Входящие данные	Математический аппарат	Выходные данные	Эконом. эффективность	Вычислит. сложность
Анализ систем состояний (переходов)	Шаблоны нормального поведения системы, шаблоны атаки	Теория графов	Вероятностная оценка реализации атаки	качественная оценка	P
Графы сценариев атак	Модель защищаемой системы, свойство корректности	Теория графов	Вероятностная оценка реализации атаки	качественная оценка	NP
Нейронные сети	Траектории в некотором числовом пространстве признаков	Алгоритмы обучения нейронных сетей	Вероятностная оценка реализации атаки	качественная оценка	P
Иммунные сети	Шаблоны нормального поведения	Специфические иммунологические теории	Вероятностная оценка реализации атаки	качественная оценка	P
Support vector machines (SVM)	Векторы признаков нормального поведения системы, шаблоны атаки	Алгоритмы обучения и переобучения	Вероятностная оценка реализации атаки	качественная оценка	NP

Экспертные системы	Факты о событиях в системе и правила вывода	Сопоставление фактов и правил	Вероятностная оценка реализации атаки	качественная оценка	NP
Основанный на спецификациях	Спецификации атак	Анализ данных	Вероятностная оценка реализации атаки	качественная оценка	NP

Окончание табл.1

Метод	Входящие данные	Математический аппарат	Выходные данные	Эконом. эффективность	Вычислит. сложность
Сигнатурный	События в системе, сигнатуры атак	Анализ данных	Вероятностная оценка реализации атаки, количественные показатели	количественная оценка	NP
Multivariate Adaptive Regression Splines (MARS)	Пространство признаков	Аппроксимация функций	Вероятностная оценка реализации атаки, количественные показатели	количественная оценка	P
Статистический анализ	Статистические данные о системе на некотором временном промежутке	Математическая статистика	Вероятностная оценка реализации атаки, количественные показатели	качественная и количественная оценка	P
Кластерный	Векторы свойств системы	Кластерный анализ	Вероятностная оценка реализации атаки, количественные показатели	качественная и количественная оценка	P
Поведенческая биометрия	Профиль нормального поведения системы	Сравнительный анализ	Вероятностная оценка реализации атаки	качественная и количественная оценка	P

Проведенный анализ систем выявления аномалий (СВА) показал, что основным недостатком подавляющего числа современных коммерческих СВА является относительно низкая эффективность обнаружения неизвестных классов кибератак [10 – 12]. При этом большинство современных СВА используют на базовом уровне ту или иную реализацию технологии сигнатурного метода обнаружения кибератак, что само по себе предусматривает организацию процесса защиты с запаздыванием. В работе [11] автор выделяет два класса методов обнаружения кибератак: методы выявления аномалий и методы выявления злоупотреблений. В обоих случаях входными данными для работы системы выступают сформированные на основе множества входных параметров шаблоны поведения – паттерны событий. Задача обнаружения кибератаки при такой постановке сводится к распознаванию шаблона поведения системы и фиксации факта ее начала. Но, как и в первом, так и во втором случаях множество входных параметров подлежит оцениванию на предмет его информативности.

В табл. 2 приведены результаты исследований некоторых методик оценки рисков. Учитывая разную природу угроз для выбранных профилей обеспечения банковской безопасности и в интересах получения в дальнейшем оценок

величины риска эквивалентного денежному капиталу, непосредственно отображающего ее защищенность предлагается использовать методики, основанные на *комплексном подходе* к оценке рисков, сочетающем количественные и качественные методы анализа, к таким относятся методики CRAMM и ФАИР, структурные схемы представлены на рис. 7, 8 (соответственно).

Таблица 2

Результаты исследований методик оценки рисков

Методика	Атрибуты							
	Качественная оценка	Количественная оценка	Комплексная оценка	Страна происхождения	Применение в банковских системах	Программная реализация	Эффективность контрмер	Простота понимания
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франция	+	+	+	-
MEHARI			+	Франция				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Германия			+	
IRAM	+			Европа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобритания	+	+	+/-	+/-
MAGERIT	+	+		Испания	+	+		
Методика НБУ	+			Украина	+		-	+

Рис. 7. Методика CRAMM – *комплексный подход* к оценке рисков

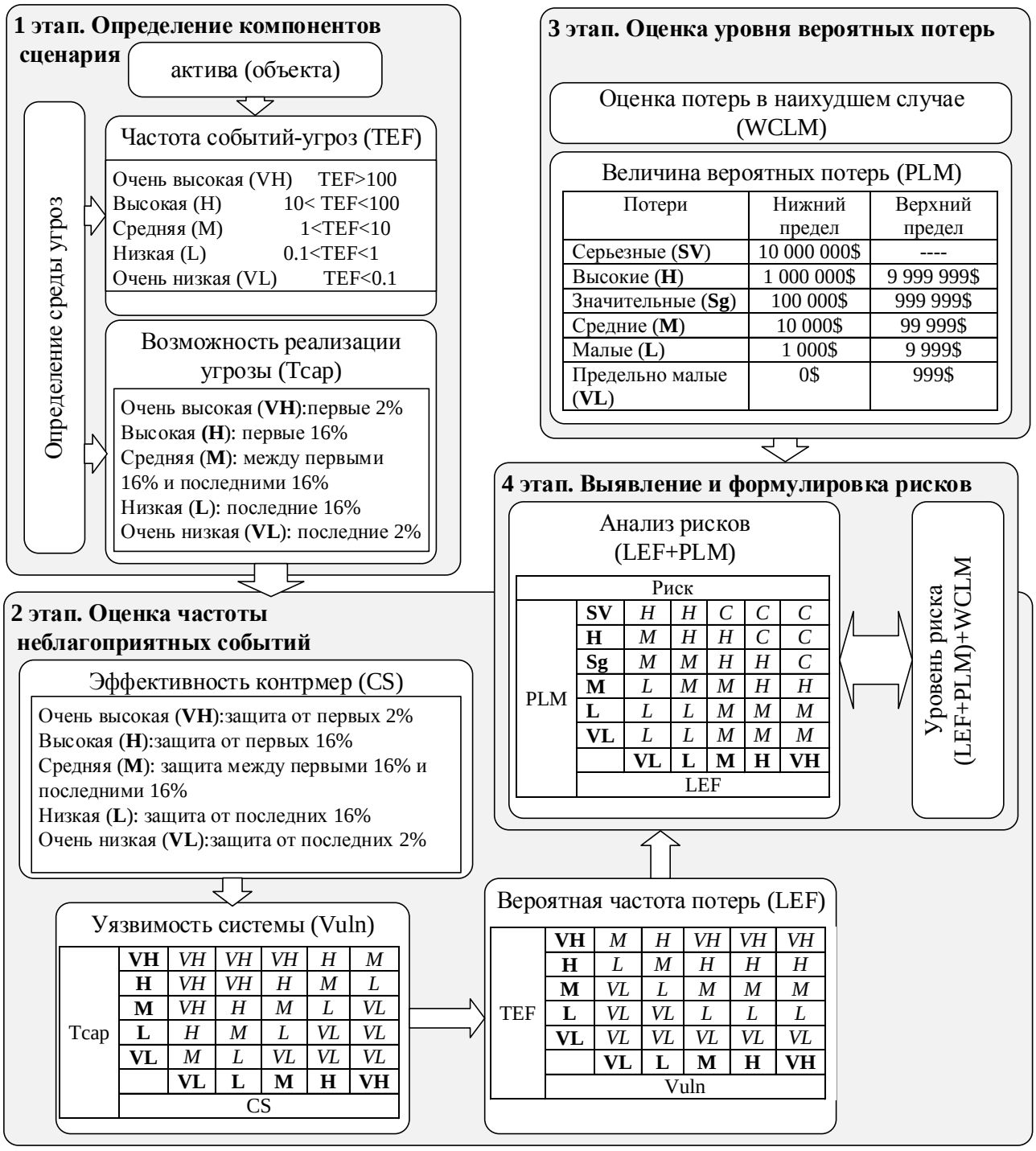

Рис. 8. Методика FAIR

Методики комплексного подхода оценки рисков, как правило, используют следующие стадии (этапы):

– на первой стадии анализируется все, что касается идентификации и определения ценности ресурсов системы: определение границ исследуемой системы: сведения о конфигурации системы, сведения об ответственных лицах за физические и программные ресурсы, определение количества пользователей системы, их привилегии. Проводится *идентификация* ресурсов: физических, программных и информационных, содержащихся внутри границ системы. Строится модель информационной системы с позиции ИБ;

– на второй стадии идентифицируются угрозы и оцениваются уровни угроз для групп ресурсов и их уязвимостей, оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы;
– третья стадия исследования заключается в поиске адекватных контрмер – поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. На этой стадии генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Взаимосвязь между методами выявления атак и методиками оценки рисков представлена на рис. 9.

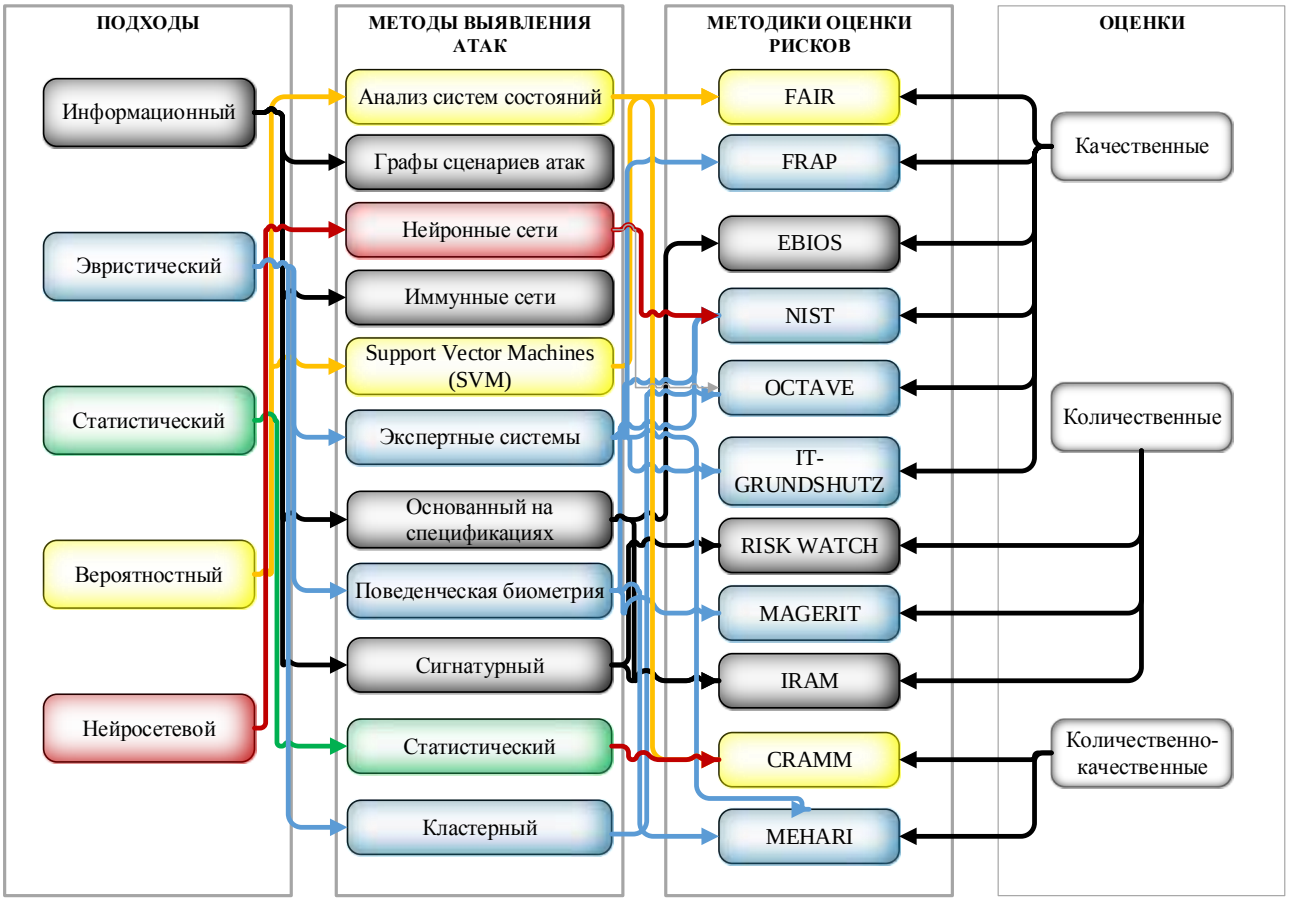

Рис. 9. Взаимосвязь между методами выявления атак и методиками оценки рисков

В контексте повышения эффективности функционирования СВА, несмотря на преимущества и недостатки каждого из направлений, они оба остаются актуальными, а потому и интенсивно развиваются. Альтернативой является дальнейшее развитие классификаторов кибератак в основу которых положены деревья принятия решений. Последние, при условии правильности их построения, дают возможность получить достаточно достоверные результаты классификации и, что характерно, имеют относительно низкую вычислительную сложность.

Важную роль в процессе классификации кибератак играют входные данные, которые выступают основой для построения классификаторов СВА коммуникационных систем. В качестве учебных и тестовых данных в представляемой работе, как и в [13], и других схожих работах, целесообразным видится применение общедоступной и широко известной базы данных KDD99. Такой подход позволят получать количественную характеристику кибератак.

Для получения качественной оценки кибератак и их дальнейшей классификации, предлагается применить известную признаковую классификацию. Такой подход позволит расширить признаковое пространство для описания неизвестных классов кибератак, структурная схема СВА, основанная на комплексировании двух известных подходов качественного и количественного приведена на рис. 10.

Рис. 10. Структурная схема СВА на основе комплексированного подхода

Таким образом, комплексирование двух известных подходов позволит объединить преимущества каждого из них, предоставляемые ними по отдельности, и при этом откроет возможности получения как количественных, так и качественных их характеристик для эффективной организации систем защиты.

Выводы. Проведенные исследования показали, что развитие вычислительных ресурсов позволили расширить спектр банковских услуг на основе использования Интернет-ресурсов. Одной из существенных проблем при проектировании и эксплуатации систем защиты банковской информации является игнорирование методологии системного анализа в отношении средств и инструментов для их защиты Задача защиты банковской информации, как правило, включает решение частных задач по обеспечению надежной и безопасной работы АБС, безопасного доступа сотрудников и клиентов к банковской системе в территориально распределенной сети, доступа сотрудников к внешним информационным сетям (Интернет-ресурсам), защиту банкоматов и терминалов, возможности контроля всех процессов в системе и

своевременного обнаружения любых нарушений.

Прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий, рост кибератак пропорционален эволюционному росту вычислительной техники в последние десятилетия и компьютерной грамотностью злоумышленников.

Проведенный анализ систем выявления аномалий (СВА) показал, что основным недостатком подавляющего числа современных коммерческих СВА является относительно низкая эффективность обнаружения неизвестных классов кибератак. С целью повышения эффективности функционирования СВА и получения как количественных, так и качественных характеристик кибератак, в данной работе предлагается комплексирование двух современных подходов: усовершенствование методов классификации кибератак на базе парадигмы искусственного интеллекта и, на их основе, алгоритмов классификации.

Проведенный анализ известных моделей анализа рисков информационной безопасности показал, что основу их составляет модель триады CIA, однако рассмотрение услуг безопасности обеспечивает сферу информационной безопасности и не позволяет комплексно оценить сферы безопасности информации и кибербезопасности АБС в режиме реального времени.

Перспективным направлением дальнейших исследований, является разработка методологии комплексирования известных классификаторов, что позволит получить новый метод выявления кибератак на ресурсы коммуникационных систем.

Литература

1. Химка, С. С. Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев [Электронный ресурс] / С. С. Химка. – Режим доступа: http://masters.donntu.org/2009/fvti/khimka/diss/index.htm

2. Украинский ресурс по безопасности [Электронный ресурс]. – Режим доступа: http://kiev-security.org.ua

3. Слободенюк, Д. Банковские технологии, Средства защиты информации в банковских системах [Электронный ресурс] / Д. Слободенюк. – 2013. – Режим доступа: http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html

4. Симаков, М. Н. V Съезд директоров по информационной безопасности [Электронный ресурс] / М. Н. Симаков. – Москва, 2012. – Режим доступа: http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf

5. Ревенков, П. В. Защита информации в банке: основные угрозы и борьба с ними [Электронный ресурс] / П. В. Ревенков. – Режим доступа: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html

6. Security of Internet Banking - A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Electronic resource].

– Available at: http://www.thailawforum.com/articles/internet-banking-thailand.html

7. Ярочкин, В. И. Информационная безопасность [Текст]: учебник / В. И. Ярочкин; 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

8. Старинський М. В. Щодо визначення поняття “банківська інформація” та виділення її видів / [Електронний ресурс]. – Режим доступу: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf

9. Евсеев С.П. Анализ законодательной базы к системе управления информационной безопасностью НСМЭП / С.П. Евсеев, О.Г. Король, Г.П. Коц. // Восточно-европейский журнал передовых технологий. – Харьков. – 2015. – Вып. 5/3(77). – С. 48-59.

10. Ленков, С. В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.

11. Сердюк, В. А. Новое в защите от взлома корпоративных систем. – Москва: Техносфера, 2007.- 360 с.

12. Мамарєв, В. М. Аналіз сучасних методів виявлення атак на ресурси інформаційно-телекомунікаційних систем [Текст] // Захист інформації, – 2011. – № 2. – С. 5 – 12.

13. Грищук, Р. В. Метод скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р. В. Грищук, В. М. Мамарєв // Сучасний захист інформації. – К. : ДУІКТ, 2012. – Спецвипуск. – С. 16–19.

14. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/v0365500-11