Техникалық шаралар әлеуетті бұзушылардың жүйенің компоненттеріне және қорғалатын ақпаратқа кіруі және қол жеткізуі мүмкін жолдарда физикалық кедергілер жасау үшін арнайы арналған әртүрлі механикалық, электр және электронды - механикалық құрылғылар мен құрылыстарды, сондай-ақ визуалды бақылау, Байланыс және күзет сигнализациясы құралдарын қолдануға негізделген. Сондай-ақ АҚ талаптарын ескере отырып, ғимараттар, құрылыстар, инженерлік коммуникациялар желілері, көлік магистральдары және т.б. салуды оңтайландыруға байланысты инженерлік-техникалық шараларды бөліп көрсетуге болады.

Бүгінгі таңда қолданыстағы бағдарламалық-техникалық шешімдерді таңдаудың барлық байлығы кәсіпорынның АҚ-ын осы деңгейде қамтамасыз ету кезінде әлі күнге дейін күрделі міндет болып қала береді . Мұның себебі мынадай бағыттар бойынша ақпараттық технологиялардың қарқынды дамуы болып табылады : жүйелердің тез әрекет етуін арттыру; желілік технологиялардың дамуы және олардың өткізу қабілетінің өсуі; қысқа мерзімде құрылған және нарықта жоғары бәсекелестікке және пайда табуына байланысты тиісті түрде қорғалмаған бағдарламалық өнімдердің айтарлықтай өсуі; жаңа ақпараттық сервистерді құру және дамыту.

Ұйымдастыру шаралары АЖ АҚ-ін қамтамасыз етуде негізгі рөл атқарады. Ұйымдастыру шаралары - бұл басқа да қорғаныс әдістері мен құралдары жоқ немесе АҚ талап етілетін деңгейін қамтамасыз ете алмайтын жалғыз нәрсе. Ұйымдастыру шаралары адамдардың қызметін регламенттеуге қатысты басқа да шараларды тиімді қолдану үшін қажет. Сонымен қатар ұйымдастыру шараларын экономикалық, инженерлік-техникалық, техникалық және бағдарламалық-аппараттық құралдармен қолдау қажет.

Қолданылған әдебиеттер тізімі

1. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы. М.: МЦПМО баспасы, 2002. 296 с.
2. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. под научн. ред. О.И. Шкартана. М.: ГУ ВШЭ, 2000. 268 с.

УДК 004.56

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МОДЕЛЬ АНАЛИЗА, КОЛИЧЕСТВЕННЫЙ И КАЧЕСТВЕННЫЙ МЕТОДЫ ОЦЕНКИ

Ким Константин Станиславович
kkimseven@gmail.com
Магистрант специальности «6М070400 – Вычислительная техника и программное обеспечение», экспериментальная образовательная программа «Администратор по управлению и защите компьютерных систем и сетей на предприятиях», факультета Информационных технологий,
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Д.Ж. Сатыбалдина

Информационная безопасность, надежность и отказоустойчивость критических инфраструктур одна из основных и приоритетных задач любой страны [1]. Растущая зависимость важных инфраструктур и промышленной автоматизации от информационных систем управления привела к многочисленным угрозам кибербезопасности. Страны во всем мире сталкиваются со сбоями и инцидентами, вызванными различными причинами в секторе основной инфраструктуры [2]. Согласно аналитическому отчету «Kaspersky lab», с 2019 по 2020 год было обнаружено и отражено свыше **975** млн. атак по всему миру, найдено около 274 млн. уникальных вредоносных объектов, что в 1.5 раз больше по сравнению с предыдущим годом [3].

В этой связи для успешной работы предприятия, необходимо определять и оценивать риски. С помощью правильной работы отдела оценки рисков, руководство может принимать корректные решения для работы и развития системы безопасности. Для промышленных систем внедрение моделей анализ рисков является инвестицией, которая обеспечит в будущем высокое качество и надежность их работы. Снижение операционных рисков и ошибок является ключом к повышению безопасности и доступности облачных сервисов [4].

Однако не существует стандартизированного метода оценки рисков для правильной оптимизации ресурсов, чтобы защитить информацию и прочие активы. В связи с этим остается актуальной задачей исследования развитие моделей рисков для новых угроз, связанных с преобладанием облачных сервисов, мобильных технологий и устройств Интернета вещей. В настоящей работе на основе литературного обзора рассмотрены модели анализа рисков и методы оценки рисков информационной безопасности (ИБ), а также исследованы, какие методы более эффективны и могут быть реализованы в проектируемом программном средстве.

Основные цели менеджмента рисков ИБ [5]:

1) мониторинг критических активов для компании, а также их эффективная защита;
2) развитие систем менеджмент ИБ;
3) поддержание эффективного принятия решений относительно политики ИБ;
4) предоставление отчетов по анализу данных для дальнейшей оценки.

Однако, для выполнения данных целей, нужно разработать эффективную, комплексную модель анализа и оценки рисков безопасности.

Анализ рисков предполагает работу в нескольких областях [6]:

– оценка вероятности (частота угрозы) должна охватывать присутствие, продолжительность и силу угрозы, а так же саму защиту и ее эффективность;
– оценка информационных, программных и аппаратных ресурсов как значимость ресурсов определяется как его стоимостью, так и последствиями от их потери;
– оценка последствий или определение степени последствий от потери определенного ресурса;
– выявление угроз как анализ угроз должен определять вероятность их возникновения и возможность потери ресурса;
– анализ восприимчивости ресурсов информационной системы.

На рисунке 1 приведены основные этапы анализа рисков ИБ в критически важных информационных инфраструктурах (critical information infrastructures, CII), предложенные авторами работы [7] на основе многокритериальных систем поддержки принятия решений (multi-criteria decision making, MCDM). В начале процесса эксперты определяют основные CII, которые требуют оценки рисков, а также угрозы, влияющие на реализацию рисков, и характеристики угроз, позволяющие выявить степень неблагоприятного воздействия реализации угрозы на CII [7].

Необходимо определить и выбрать метод оценки рисков (количественный и/или качественный), чтобы затем их ранжировать и начать смягчать наиболее опасные из них.

Целью количественного подхода является вычисление числовых значений, связанных с каждым компонентом. Примеры количественных методов: ГРУ, методы Кортни и Фишера, модель ISRAM и т. д. Оценивается реальная стоимость активов с учетом стоимости замены, стоимость потери производительности, стоимость ущерба репутации бренда и другие ценности, которые представляют собой прямые или косвенные активы для организации. Количественный подход к риску состоит из нескольких шагов, которым необходимо следовать. На первом этапе активы компании идентифицируются и оцениваются с целью оценки потенциальных убытков в случае атаки. Стоимость восстановления или замены должна быть установлена в случае частичного или полного уничтожения актива. Каждый актив в случае потери, оказывает влияние на один из трех основных элементов, необходимых для обеспечения безопасности: конфиденциальность, целостность и доступность. Далее

годовой расчетный убыток (ГРУ) может быть рассчитан как сумма стоимости каждого затронутого актива, взвешенная с частотой появления каждой угрозы. Последний шаг в количественном анализе дохода от инвестиций (ДОИ), а так же состоит в определении мер, которые должны быть реализованы.

На этом этапе выявляются угрозы, которые создают наибольшие убытки (ГРУ) и меры, которые должны быть реализованы для уменьшения потерь. Для каждой меры определяется [5]:

1) угрозы, которые могут быть устранены путем реализации меры;
2) годовой расчетный убыток для каждой угрозы;
3) показатель эффективности меры;
4) доход от инвестиций (ДОИ).

Качественные методики оценки рисков не оперируют числовыми данными, представление результатов для них в виде описаний, рекомендации, Оценка рисков в этом случае связана со следующими действиями:

– качественное описание стоимости активов, определение качественных шкал для частоты угрозы возникновение и подверженность данной угрозе;

– описание так называемых сценариев угроз с помощью прогноза из основных факторов риска.

Примеры количественных методов: FMEA / FMECA, Microsoft Corporate Security Group Risk Management Framework, NIST SP 800-30, CRAMM.

Качественные методы в основном используется небольшими организациями. Они не используют статистические значения, чтобы оценить риск. Вместо этого, значения относительные значения используются как входные данные для значения потенциальных потерь. Метод может быть применен путем выполнения следующих этапов:

1) определение уровня потерь;
2) определение затрат инцидента;
3) определение частоты возникновения инцидента;
4) определение последствий инцидента;
5) определение качественной матрицы анализа рисков.

Количественные и качественные методы являются двумя основными группами методов анализа рисков, которые применяются на сегодняшний день. В таблице 1 представлены преимущества и недостатки каждого из подходов [8].

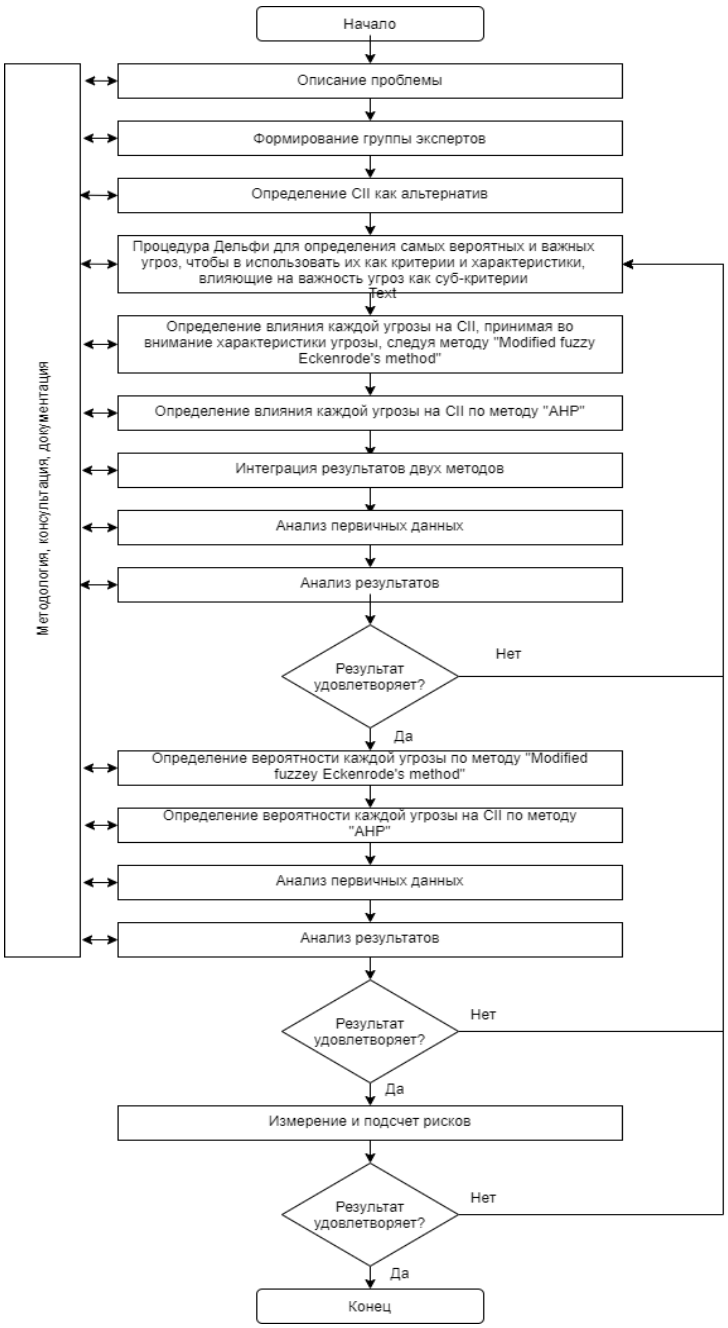

Рисунок 1. Модель управления рисками ИБ [6]

Таблица 1. Сравнение качественного и количественного методов оценки рисков ИБ

Анализ рисков	Преимущества	Недостатки
Количественные	- Они позволяют определить последствия инцидентов в количественном выражении, что облегчает реализацию анализ затрат и выгод при выборе средств защиты. - Они дают более точное представление о риске	- Количественные показатели зависят от объема и точности определяет шкалу измерения. - Результаты анализа могут быть не точными и даже запутанными. - Нормальные методы должны быть обогащены в качественном описании (в форме комментария, интерпретации) [9]. - Анализ, проведенный с применением этих методов, как

		правило, дороже, требует большего опыта и продвинутые инструменты.
Качественные	- Это позволяет упорядочить риски в соответствии с приоритетом. - Это позволяет определить зоны повышенного риска в короткой время и без больших затрат. - Анализ относительно прост и дешев [9].	- Не позволяет определять вероятности и результаты используя числовые меры. - Анализ затрат и выгод более сложен при выборе защита. - Достигнутые результаты носят общий характер, приблизительный и т. д.

Описанные выше модели и методы управления рисками безопасности охватывает ряд стандартов и методов для защиты традиционных активов и управления безопасностью. Однако современные тенденции развития IT – технологий требуют учета особенностей рисков, связанных с мобильными устройствами, объектами IoT - систем. Поскольку в настоящее время все чаще используется модель *BYOD (*bring your own device), бизнес пользователям предоставляется доступ на высоком уровне с персональных мобильных устройств, смартфоны и планшеты эффективно заменяют рабочие столы для многих бизнес задач. Однако персональные мобильные устройства не обеспечивают такой же уровень встроенной безопасности или контроля, как настольные компьютеры, принадлежащие организации, которые они заменяют. При этом угрозы безопасности мобильных устройств растут. В 2014 году Kaspersky обнаружил почти 3,5 миллиона вредоносных программ на более чем 1 миллионе пользовательских устройств, к 2017 году технология обнаружения в лаборатории «Лаборатории Касперского» достигла 360 000 вредоносных файлов в день [10]. И 78% этих файлов были вредоносными программами, что означает, что в день выявлялось более 280 000 вредоносных файлов, многие из которых предназначены для мобильных устройств [11].

В связи с вышесказанным, следующей задачей научного исследования в рамках темы магистерской диссертации является разработка базы знаний по угрозам, связанным с использованием мобильных устройств, идентификация соответствующих для них уязвимостей, развитие количественного, качественного или гибридного метода и программная реализация модели анализа и оценки рисков ИБ.

Список использованных источников

1. Kaklauskas, A., Dzemyda, G., Tupenaite, L., Voitau, I., Kurasova, O., Naimaviciene, J., Rassokha, Y., Kanapeckiene, L. Artificial neural network-based decision support system for development of an energy efficient built environment// Energies. -2018.- Pp.344-400.
2. Miao, X., Yu, B., Xi, B., Tangd, Y.H. Modeling of bilevel games and incentives for a sustainable critical infrastructure system. //Technological and Economic Development of Economy.- 2010.- V. 16(3).- Pp.365–379.

3. Kaspersky Security Bulletin 2019. Статистика. Available online: https://securelist.ru/ kaspersky-security-bulletin-2019-statistics/95264/ (accessed on 24 March 2020).
4. Hu, K.H., Jianguo, W., Tzeng, G.H. (2017). Risk factor assessment improvement for China's cloud computing auditing using a new hybrid MADM model. // International Journal of Information Technology & Decision Making.- V. 16(03).- Pp.737–777.
5. Artur Rot. IT Risk Assessment: Quantitative and Qualitative Approach// Lecture Notes in Engineering and Computer Science. – 2008.- V.2173. - Pp. 1-6.
6. Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim. A Security Risk Analysis Model for Information Systems // Systems modeling and Simulation: Theory and Applications: Third Asian Simulation Conference.- Pp. 1-4.- 2004
7. Turksis Z., Goranin N., Nurusheva A., Boranbayev S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. // INFORMATICA.- 2019.- Vol. 30, No. 1.- Pp. 187-211.
8. Stroie E. R. Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. // Chinese Business Review.- Pp. 1-3. -2012. –Vol. 10, No. 12, 1106-1110

9. Todd D. Jick Mixing Qualitative and Quantitative Methods: Triangulation in Action // Administrative Science Quarterly, Vol. 24, No. 4, Qualitative Methodology (Dec., 1979), Pp. 602-611.- 2011
10. Kaspersky Lab. Top 7 Mobile Security Threats in 2020. Available online: https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (accessed on 24 March 2020)
11. Kaspersky Lab Mobile Malware Continues to Grow and Online Bank Accounts are Targeted More Than 5 Million Times, Kaspersky Lab Q3 Report Shows. Available online: https://www.kaspersky.com/about/press-releases/2015_mobile-malware-continues-to-grow-and-online-bank-accounts-are-targeted-more-than-5-million-times-kaspersky-lab-q3-report-shows (accessed on 24 March 2020)

УДК 004

ОБНАРУЖЕНИЕ SINKHOLE - АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Марденов Ерік Маратұлы
uvideooperator@mail.ru
Докторант ФИТ ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Т.К.Жукабаева

Аннотация. Беспроводные сенсорные сети (БСС) подвержен многочисленным типам угроз и атак. Эта статья посвящена одной из сложных атак маршрутизаций – Sinkhole атака, которая является одной из самых строгих атак маршрутизации, поскольку она привлекает окружающие узлы вводящей в заблуждение информацией о маршруте и выполняет подделку данных или выборочную пересылку данных, проходящих через него.

Ключевые слова: Беспроводная сенсорная сеть, Sinkhole атака, Защитные атаки, Специальная сеть, Обнаружение вторжений.

Введение

С развитием технологий растет интерес к использованию БСС. Это область, где активные исследования могут проводиться с использованием различных алгоритмов, моделей, факторов безопасности и социальных факторов[1]. БСС представляют собой комбинацию чувствительных узлов и отвечают за восприятие, а также за первые этапы иерархии обработки[2].

Безопасность - жизненно важная проблема в БСС. Многие исследования сосредоточены на предоставлении решений безопасности для этих сетей