УДК 004.056 Вестник УрФО № 4(46) / 2022, с. 26–31

Маслова М.А.

DOI: 10.14529/secur220403

ПРОГРАММНЫЕ МЕТОДЫ ВЫРАБОТКИ РЕКОМЕНДАЦИЙ ПРИ ЭКСПЕРТНОМ АУДИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Проведение экспертной оценки при анализе и оценке рисков информационной безопасности является одним из актуальных и постоянно применяемых методов в организациях. Получение грамотных составленных рекомендаций, относящихся непосредственно к рассматриваемому направлению работы организации есть одним из залогов уменьшения и предупреждения возможных рисков. В данной работе будет рассмотрены и приведены составленные уникальные рекомендации для входных параметров, выделенных и объединенных в одну большую базу данных из уже применяемых методик, на основе рассмотренных методов анализа и оценки рисков информационной безопасности в работах [1 3], а также нормативных актов, законодательной базы и необходимых мер по обнаружению, предупреждению и устранению рисков информационной безопасности в организациях.

Ключевые слова: *рекомендации, риски информационной безопасности, входные данные, анализ и оценка рисков информационной безопасности.*

Maslova M.A.

PROGRAM METHODS FOR DEVELOPING RECOMMENDATIONS IN EXPERT AUDIT OF INFORMATION SYSTEMS

Conducting peer review in the analysis and assessment of information security risks is one of the relevant and constantly used methods in organizations. Obtaining competently compiled recommendations related directly to the considered direction of the organization's work is one of the keys to reducing and preventing possible risks. In this paper, unique recommendations will be considered and presented for input parameters selected and combined into one large database from already used methods, based on the considered methods for analyzing and assessing information security risks in [1 3], as well as regulations, the legal framework and the necessary measures to detect, prevent and eliminate information security risks in organizations.

Keywords: *recommendations, information security risks, input data, analysis and assessment of information security risks.*

Процесс управления рисками информационной безопасности (ИБ) в России набирает все большее значение и становится системным и формализованным, появляются новые программные средства, с помощью которых можно автоматизировать процессы оценки и анализа рисков ИБ и принимаются новые стандарты и методы с грамотным описанием алгоритмов управления рисками. Недостатки в них есть, так как нет полностью комплексного подхода, который бы рассматривал и нормативно-технические, и организационные, и технические меры защиты одновременно [4 - 7].

Но прогресс не стоит на месте и постоянно появляются и усовершенствуются существующие методы оценки и анализа рисков ИБ.

В данной работе будет рассматриваться разрабатываемый программный модуль для анализа и оценки рисков ИБ в организации, который позволит проработать большую базу входных данных и с помощью метода экспертных оценок получить рекомендации по их устранению и предотвращению.

Метод экспертных оценок является одним из самых распространенных и часто применяемых методов оценки рисков.

После проведения метода экспертных оценок в результате выдаются рекомендации по принятию, предупреждению, устранению выявленных рисков для организаций, где решающую роль в данном процессе уже определяет руководство организации для которой проводилась экспертиза. Так как эксперты не могут на 100% дать правильные ответы и выводы из-за различных скрытых аспектов, неучтенных факторов, существующих в организации [8 - 10].

В разрабатываемом программном модуле были определены входные и выходные параметры анализируемых методик анализа и оценки рисков информационной безопасности: CORAS, Risk IT, ГРИФ, MSAT, СТО БР ИББС, CRAMM, MOF, Risk Watch, OCTAVE, FRAP, ISO/IEC 27001 [2]. Далее на основе метода Дельфи проводится экспертная оценка и рассчитаны параметры сходимости, которые выдаются в числовом значении от главного до не значащего параметра риска [8]. В итоге по каждому значению выдается составленная рекомендация для уменьшения, устранения риска.

Рассмотрим примеры некоторых рекомендаций для входных параметров:

1) Программное обеспечение:

– Применение специальных алгоритмов и компонент для программного обеспечения для контроля, защиты от НСД и разграничения доступа;

– Защита программного обеспечения от атак, модификаций, хищения, редактирования и разрушения с помощью шифрования, алгоритмов запутывания и обфускации, эмуляция процессов и методы периодической проверки программного кода и целостности данных;

– Установка парольной защиты на запуск с ограничениями и разграничением прав доступа пользователей, использование ключевых флешек для работы и запуска программ;

– Регулярное обновление базы данных, программ и программных модулей с помощью защиты криптографическими методами;

– При установки нового программного обеспечения необходимо получать доступ у руководства, с подтверждением их цели и использования для поддержания среды безопасности локальной информационной системы с соблюдением политики безопасности предприятия;

– Проводить проверку на совместимость с различными компонентами системы аппаратные и программные средства;

– Проводить анализ всех функциональных системных и интерфейсных требований необходимых для программной реализации на отсутствие неопределенностей, противоречий и несоответствий;

– Регистрировать и вести журнал учета по выявленным недочетам, исправлениям, несоответствиям и неопределенностям входной информации;

– Контроль спецификации в документе требований для верхнего уровня установленных системных требований для реализации программного процесса;

– Для предотвращения риска необходимо определить требования для верхнего уровня с учетом установленных системных требований;

– Проводить оценку безопасности системы производных требований верхнего уровня [11].

2) Конкурентное преимущество:

– Наличие в организации квалифицированного работника;

– Проведение постоянного аудита рынка относящиеся к конкурентам;

– Мониторинг и составление отчетов отношения базовых показателей к достигнутым успехам, промежуточных, полных и итоговых отчетов организации;

– Составление отчетов по главным параметрам: финансирование, инвестиции, затраты на рекламу и дополнительную раскрутку, оценка рисков по разным параметрам и т.д.;

– Постоянный (установленный период в организации) по мониторингу безопасности к различным значимым критериям: программное обеспечение, персонал, процессы, технологии и т.д.;

– Создание полного отчета организации на основе промежуточных, раз в квартал по увеличению результативности и уровня безопасности.

3) Атаки злоумышленников (взломы, DDOS):

– Периодическое обновление операционной системы;

– Использование лицензированного программного обеспечения;

– Установка и постоянное обновление антивирусов, имеющих встроенную изолированную среду;

– Установка межсетевых экранов и сервисов анти-DDoS;

– Установка паролей относящимся к сложным и смена их не менее чем раз в три месяца;

– Применение SIEM-решений;

– Установка двухфакторной аутентификации;

– Ежемесячное проведение тестирования на проникновения и анализ защищенности Web-приложений;

– Составление отчетов об угрозах, мерах их устранения и уровню безопасности;

– Разработка планов и стратегий по улучшению безопасности учитывая показатели рисков, их оценку, изменение и устранение [12, 13].

4) Неумышленное раскрытие сотрудниками конфиденциальной информации:

– Постоянный мониторинг возможных нежелательных инцидентов, угроз и уязвимостей;

– При приеме на работу сотрудников подписывать документ о неразглашении конфиденциальной информации;

– Проведение периодических инструктажей о рисках, угрозах, потерях, возможных последствиях при разглашении конфиденциальной информации;

– Доведение до сотрудников мер и возможных наказаний по гражданско-правовой, административной, дисциплинарной и уголовной ответственности;

– Оценка и составление отчетностей по возможным нежелательным инцидентам и вероятностям их возникновения;

– Оценка ущерба, возникшего из-за потери или утечки персональных данных определенных лиц;

– Анализ имеющихся информационных рисков, их градация, частота повторения и влияние на работу системы организации;

– Разработка и рекомендации по действиям во время восстановления работоспособности и их постоянного обновления;

– Выявления и просчет потерь связанных с выполнением обязанностей сотрудников;

– Оценку рисков проводить, используя разные подходы: на начальном этапе – качественным методом, на заключительном – количественным [14].

5) Преднамеренное несанкционированное действие сотрудников:

– Постоянный контроль 24/7, выявление и прогнозирование угроз, возможных условий и причин, по которым производится ущерб заинтересованными пользователями по функционированию информационной системы организации;

– Вход / выход сотрудников осуществляется по пропускам в организацию, вход в систему организации осуществляется по логинам и паролям, имеющим соответствующую защиту и сложность доступа, подбора и взлома;

– Проверка и контроль входа/ выхода сотрудников, внос и вынос имущества;

– Для важных объектов ввести контроль входа с дополнительными параметрами аутентификации пользователя;

– Проводить периодические встречи по повышению квалификации, доведения инструкций по грамотному использованию системы, хранению, составлению и смене паролей;

– Проводить повышение квалификации для администраторов и сотрудников, отвечающих за безопасность организации;

– При приеме на работу тщательная проверка и отбор сотрудников;

– Постоянный подбор кадров для резерва;

– Смена всех паролей и лишения прав доступа пользователя при увольнении с работы;

– Мониторинг и выявление потенциальных угроз нарушения целостности, конфиденциальности и доступности;

– Мониторинг и разработка мер по снижению и ликвидации потенциальных угроз как для кратковременных, так и долговременных перспектив организации;

– Составление и просчет финансовых затрат и потерь от разглашения данных, информации, репутации и др. важных параметров организации;

– Составление матрицы угроз и мер по предотвращению и ликвидации [15].

6) Доступ к сетям и сетевым службам:

Выделяют требования по безопасности:

– Идентификацию и аутентификацию пользователей;

– Грамотное управление доступом к системам по времени, местоположению, доверенным маршрутом, количеством неудачных входов, разграничения действий между субъектами;

– Отказ в доступе неавторизированного персонала;

– Контроль процесса ввода и обработки данных с последующим корректным их завершение на выходе;

– При создании политики безопасности организации необходимо учитывать следующие параметры и правила:

– Установление требований к безопасности используемых прикладных программ и рисков, касающихся их;

– Установить принципы, уровни безопасности и классификации по распространению информации;

– Установить согласованность между управлением доступа и политикой классификации информации для различных сетей и систем;

– Применять полное соответствие и требования нормативной документации для защиты доступа к данным или услугам;

– Установить стандартные профили доступа относительно пользователей для должностных руководств;

– Установить менеджмент прав доступа в распределенной среде или сетях, учитывая всевозможные типы доступных соединений;

– Установка распределения ролей управления доступом с запросом на доступ и возможностью периодического пересмотра к доступу и его аннулированию.

Политика должна действовать для: сетей и сетевых сервисов к которым разрешен доступ; к процедурам авторизации; мерам их управления и защиты доступа к сетевым соединениям и сетевым сервисам; средства, используемые для доступа к данным сетям и сетевым сервисам; требований аутентификации пользователя по доступу к разным сетевым сервисам и их мониторингу; принятия быстрых и четких решений по внедрению новых мер, механизмов безопасности новых или модификации старых учитывая их приемлемость, затраты и последующую выгоду; составления списка рекомендаций по улучшению и модификации мер и процедур управления и контролем непосредственно влияющих на информационную безопасность [16, 17].

Выводы

В данной работе были рассмотрены и приведены выборочные составленные уникальные рекомендации для входных параметров, применяемых для анализа и оценки угроз информационной безопасности описанных в предыдущих работах, основанные на уже применяемых в мире методах для анализа и оценки рисков информационной безопасности, а также нормативных актах, законодательной базы и необходимых мер по обнаружению, предупреждению и устранению рисков информационной безопасности в организациях. С помощью составленной расширенной базы рекомендаций для ста восьмидесяти четырех входных параметров экспертам предоставляется возможность тщательнее и глубже проработать всевозможные рисковые ситуации и пути их решения для оцениваемой организации.

Благодарность. Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

Литература

1. Маслова, М. А. Сравнительный анализ методов оценки рисков информационной безопасности, основанных на стандартных и интеллектуальных подходах / М. А. Маслова, Е. Н. Тищенко // Про-

блемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики: материалы XIX Международной научно-практической конференции, Ростов-на-Дону, 28–29 октября 2019 года / Ростовский государственный экономический университет (РИНХ). – Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ», 2019. – С. 211-215.

2. Маслова, М. А. Анализ сходимости входных данных для методик оценки рисков информационной безопасности / М. А. Маслова, Н. С. Смирнов // Современные проблемы радиоэлектроники и телекоммуникаций. – 2021. – № 4. – С. 215.

3. Маслова, М. А. Инструментальный подход к оценке рисков информационной безопасности / М. А. Маслова // Информация и безопасность. – 2022. – Т. 25. – № 2. – С. 209-216.

4. Анализ рисков информационной безопасности URL: taxpravo.ru/analitika/statya-131560-naliz_riskov_informatsionnoy_bezopasnosti.html (дата обращения 26.04.2022).

5. Макарова, О. С. Методика прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя / О. С. Макарова, С. В. Поршнев // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1(43). – С. 64-73.

6. Минбалеев, А. В. Проблемы и перспективы обеспечения защиты персональных данных граждан в цифровом профиле / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 4(42). – С. 59-63.

7. Риски информационной безопасности | Управление рисками информационной безопасности URL: https://www.dialognauka.ru/press-center/article/5990/?ysclid=laxz579slh74947120 (дата обращения 16.10.2022).

8. Маслова, М. А. Анализ, применение и модификация метода Дельфи / М. А. Маслова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2(44). – С. 25-29.

9. Санжапов, Б. Х. Метод принятия решений на основе многокритериальных распределенных экспертных оценок / Б. Х. Санжапов, И. С. Калина // Прикаспийский журнал: управление и высокие технологии. – 2008. – № 2(2). – С. 62-67.

10. Федоров, В. А. Метод экспертных оценок как способ оценки риска / В. А. Федоров, Е. Н. Маковеева // Развитие науки и техники: механизм выбора и реализации приоритетов: сборник статей Международной научно-практической конференции: в 3 частях, Екатеринбург, 15 июня 2017 года. Том Часть 1. – Екатеринбург: Общество с ограниченной ответственностью «Аэтерна», 2017. – С. 146-148.

11. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

12. ФСТЭК РОССИИ. «МЕТОДИЧЕСКИЙ ДОКУМЕНТ. Методика определения безопасности информации в информационных системах».

13. ГОСТ Р ИСО/МЭК 27033-3-2014. «НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. Information technology. Security techniques. Network security. Part 3. Reference networking scenarios. Threats, design techniques and control issues».

14. ГОСТ Р 51275-99 Группа Э00 «Государственный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatization. Factors influencing the information. General outlines».

15. ГОСТ Р 51904-2002 «Государственный стандарт Российской Федерации. Программное обеспечение встроенных систем. Общие требования к разработке и документированию. Embedded system software. General requirements for development and documentation».

16. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».

17. ГОСТ Р 57628— 2017 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

References

1. Maslova, M. A. Sravnitel'nyy analiz metodov otsenki riskov informatsionnoy bezopasnosti, osnovannykh na standartnykh i intellektual'nykh podkhodakh / M. A. Maslova, Ye. N. Tishchenko // Problemy proyektirovaniya, primeneniya i bezopasnosti informatsionnykh sistem v usloviyakh tsifrovoy ekonomiki: materialy XIX Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Rostov-na-Donu, 28–29 oktyabrya 2019 goda / Rostovskiy gosudarstvennyy ekonomicheskiy universitet (RINKH). – Rostov-na-Donu: Rostovskiy gosudarstvennyy ekonomicheskiy universitet "RINKH", 2019. – S. 211-215.

2. Maslova, M. A. Analiz skhodimosti vkhodnykh dannykh dlya metodik otsenki riskov informatsionnoy

bezopasnosti / M. A. Maslova, N. S. Smirnov // Sovremennyye problemy radioelektroniki i telekommunikatsiy. – 2021. – № 4. – S. 215.

3. Maslova, M. A. Instrumental'nyy podkhod k otsenke riskov informatsionnoy bezopasnosti / M. A. Maslova // Informatsiya i bezopasnost'. – 2022. – T. 25. – № 2. – S. 209-216.

4. Analiz riskov informatsionnoy bezopasnosti URL: taxpravo.ru/analitika/statya-131560-naliz_riskov_informatsionnoy_bezopasnosti.html (data obrashcheniya 26.04.2022).

5. Makarova, O. S. Metodika prognozirovaniya dinamiki veroyatnosti provedeniya komp'yuternoy ataki s tochki zreniya narushitelya / O. S. Makarova, S. V. Porshnev // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2022. – № 1(43). – S. 64-73. 6. Minbaleyev, A. V. Problemy i perspektivy obespecheniya zashchity personal'nykh dannykh grazhdan v tsifrovom profile / A. V. Minbaleyev // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – № 4(42). – S. 59-63.

7. Riski informatsionnoy bezopasnosti | Upravleniye riskami informatsionnoy bezopasnosti URL: https://www.dialognauka.ru/press-center/article/5990/?ysclid=laxz579slh74947120 (data obrashcheniya 16.10.2022).

8. Maslova, M. A. Analiz, primeneniye i modifikatsiya metoda Del'fi / M. A. Maslova // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2022. – № 2(44). – S. 25-29. 9. Sanzhapov, B. KH. Metod prinyatiya resheniy na osnove mnogokriterial'nykh raspredelennykh ekspertnykh otsenok / B. KH. Sanzhapov, I. S. Kalina // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. – 2008. – № 2(2). – S. 62-67.

10. Fedorov, V. A. Metod ekspertnykh otsenok kak sposob otsenki riska / V. A. Fedorov, Ye. N. Makoveyeva // Razvitiye nauki i tekhniki: mekhanizm vybora i realizatsii prioritetov: sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii: v 3 chastyakh, Yekaterinburg, 15 iyunya 2017 goda. Tom Chast' 1. – Yekaterinburg: Obshchestvo s ogranichennoy otvetstvennost'yu "Aeterna", 2017. – S. 146-148.

11. GOST R ISO/MEK 27002-2012 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoy bezopasnosti».

12. FSTEK ROSSII. «METODICHESKIY DOKUMENT. Metodika opredeleniya bezopasnosti informatsii v informatsionnykh sistemakh».

13. GOST R ISO/MEK 27033-3-2014. «NATSIONAL'NYY STANDART ROSSIYSKOY FEDERATSII. Informatsionnaya tekhnologiya. METODY I SREDSTVA OBESPECHENIYA BEZOPASNOSTI. Bezopasnost' setey. Chast' 3. Etalonnyye setevyye stsenarii. Ugrozy, metody proyektirovaniya i voprosy upravleniya. Information technology. Security techniques. Network security. Part 3. Reference networking scenarios. Threats, design techniques and control issues».

14. GOST R 51275-99 Gruppa E00 «Gosudarstvennyy standart Rossiyskoy Federatsii. Zashchita informatsii. Ob"yekt informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya Protection of information. Object of informatization. Factors influencing the information. General outlines».

15. GOST R 51904-2002 «Gosudarstvennyy standart Rossiyskoy Federatsii. Programmnoye obespecheniye vstroyennykh sistem. Obshchiye trebovaniya k razrabotke i dokumentirovaniyu. Embedded system software. General requirements for development and documentation».

16. GOST R ISO/MEK 27002-2021 «Informatsionnyye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil primeneniya mer obespecheniya informatsionnoy bezopasnosti».

17. GOST R 57628— 2017 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Rukovodstvo po razrabotke profiley zashchity i zadaniy po bezopasnosti».

МАСЛОВА Мария Александровна, старший преподаватель кафедры «Информационная безопасность» Федеральное государственное автономное образовательное учреждение высшего образования Севастопольский государственный университет. Россия, 299053, г. Севастополь, Университетская улица, дом 33; аспирант, м.н.с. Федеральное государственное автономное образовательное учреждение высшего образования Ростовский государственный экономический университет (РИНХ). Россия, 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E–mail: mashechka–81@mail.ru

MASLOVA Maria Aleksandrovna, Senior Lecturer of the Information Security Department Federal State Autonomous Educational Institution of Higher Education Sevastopol State University. Universitetskaya street, 33, Sevastopol, 299053, Russia; postgraduate student, junior researcher Federal State Autonomous Higher Educational Institution Rostov State University of Economics (RINH). st. Bolshaya Sadovaya, 69, Rostov-on-Don, 344002, Russia. E-mail: mashechka–81@mail.ru;