DOI 10.36622/VSTU.2022.25.4.005
УДК 004.056

НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕГУЛИРОВАНИЮ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. Маслова

В статье рассмотрены научно методические рекомендации, касающиеся регулирования рисков информационной безопасности. Исследование содержит обобщение работ автора по анализу и управлению рисками, связанными с информационной безопасностью. Предлагается модификация методики Дельфи, реализованная и исследованная в виде программного прототипа. Анализ сходимости результатов предложенной методики сопоставляется с данными и методиками: MOF, MSAT, CRAMM, Risk IT, ГРИФ, OCTAVE, FRAP, CORAS, СТО БР ИББС, Risk Watch. Методика предполагает создание расширенной базы данных параметров из вышеуказанных методик с возможностью ее последующей модификации и дополнения, а также с рекомендациями на выходе для принятия эффективных управленческих решений, снижения и ликвидации рисков информационной безопасности для минимизации потерь предприятия.

Ключевые слова: риски информационной безопасности, уязвимости, снижение рисков информационной безопасности, рекомендации, методики.

Введение

Рискам информационной безопасности необходимо уделять достаточно много времени на предприятии, постоянно их анализировать и контролировать, так как их оценка позволяет в дальнейшем упростить выполнение задач и всю дальнейшую деятельность на предприятии. Необходимо определить все стадии оценки рисков от определения объекта оценки до выделения выходных данных и рекомендаций [1-3].

Так как большое значение имеют параметры и влияющие на них источники угроз внутренние и внешние, то оценку желательно проводить комплексную. Самыми часто используемыми методиками информационной безопасности для оценки рисков в мире являются методики:

- FRAP,
- OCTAVE,
- CRAMM,
- Microsoft,
- COBIT of Risk.

Все существующие методики не проводят полную и исчерпывающую оценку рисков информационной безопасности, а определяют некоторые конкретные параметры. Они в основном используются в коммерческих целях, а для государственных предприятий необходимо обязательно учитывать и применять положения нормативных актов ФСТЭК России.[4]

С развитием информационных технологий увеличилось количество атак и уязвимостей системы, поэтому стало острой задачей необходимость обязательного применения качественной, своевременной, регулярной защиты существующих систем на предприятиях. Применение качественной защиты, постоянный мониторинг и поиск «дырок», наличие всевозможных рисков из-за которых предприятия терпят убытки стало важным элементов функционирования любой системы предприятия [4-6].

Какое бы ни было предприятие или коммерческая компания все они стремятся к успешной, стабильной работе с достижением определенных целей, но не зависимо от того на что направлено действие предприятия или компании - это есть финансовый доход или предоставление услуг в разных сферах. Если не обращать внимание, не просчитывать и не снижать риски информационной безопасности, то достигнуть результата будет не возможным. Понятно, что полностью от рисков избавиться невозможно, но необходимо обязательно направлять действия на их снижение до приемлемого уровня в организации. Достижение данного результата становиться возможным благодаря комплексным системам информационной безопасности. Благодаря постоянному мониторингу и анализу рисков

информационной безопасности предприятие может снизить свои затраты и максимально эффективно определить и создать всю совокупность средств защиты информации и определить организационные меры, направленные на уменьшение рисков информационной безопасности.

Предлагаемая методика позволить укрупнить данную базу данных и использовать ее для разносторонних предприятий.

Основная часть

Разрабатываемая методика анализа и оценки рисков информационной безопасности позволяет на начальном этапе экспертам, которые будут проводить экспертизу ознакомиться с заказчиком (предприятием) благодаря заполненной форме на проведение экспертизы, его параметрами и пожеланиями к каким-то важным параметрам для предприятия, на которые акцентирует ответственное лицо заказывающее экспертизу. После эксперты приступают к оценке важности параметров по шкале от 0 до 10, которые были выделены из основных применяемых методик анализа и оценки рисков информационной безопасности:

– СТО БР ИББС,
– Risk Watch,
– MOF,
– MSAT,
– CRAMM,
– Risk IT,
– ГРИФ,
– OCTAVE,
– FRAP,
– CORAS,

рассмотренных в статье [3].

Так же были выделены параметры выходных данных, после сопоставлены с входными данными. Далее по методу Дельфи просчитаны сходимости параметров, выявлен перечень важности входных и выходных параметров и по уже полученным данным составляются рекомендации для определенного актива информационной безопасности по снижению и предотвращению рисковых ситуаций.

Также обязательно при составлении рекомендаций необходимо руководствоваться действующими нормативными актами и законодательной базой.

Рассмотрим некоторые полученные параметры проделанной работы:

– При нарушении конфиденциальности при НСД выходными данными будут являться:

– Оценка последствий, возникающие при осуществлении нежелательных инцидентов и их вероятностей;

– Оценка ущерба, который может возникнуть и вероятность его осуществления нежелательных инцидентов и их вероятностей;

– Составление списков уязвимостей, которые необходимо устранить в ближайшее время;

– Существующие угрозы с помощью которых происходит нарушение: доступности, целостности, конфиденциальности, а также вероятности возможной их реализации;

– Нанесение убытков от реализации основной деятельности предприятия;

– Выявление всех возможных потенциальных нежелательных инцидентов, возможных предполагаемых угроз, уязвимостей.

– Оценка потерь от угроз: финансовых, репутационных, дающих сбои при работе системы, промежуточных и годовых;

– Создание отчетов: стоимость приобретенных защищаемых ресурсов; возможных потерь от угроз; текущего уровня состояния безопасности и др. важных параметров организации; финансовых потерей при разглашении информации и утечки личных данных;

– Углубленный анализ и составление списка основных рисков, которые необходимо постоянно мониторить, следить за ними и быстро устранять с определением мер защиты;

– Расставление по приоритетности действий для улучшения безопасности;

– Составление рекомендаций к действиям в случае возникновения рискового события;

– Проведения анализа физической защиты информационной системы;

– Отчеты по оценки ущерба для:

персонала, при разглашении ПДн;

– Составление целостного подхода к изменению уровня безопасности как для процессов и технологий, так и для персонала предприятия.

– Рекомендации для данных параметров:

– Применение контроля доступа от НСД пользователей и лиц, имеющих доступ к различным устройствам;

– Создание резервных копий файлов, системы на съемных носителях, на облачных сервисах с применение многоуровневой защиты;

– Применение и постоянное обновление лицензированной антивирусной защиты;

– Применение и постоянное обновление лицензированных программ для работы на предприятии.

1) Сервера и устройства хранения данных - выходными данными будут являться:

– Создание отчетов о рассматриваемой системе и ее характеристики;

– Проведение периодической оценки уровней рисков для системы и разработка существующих показателей ИС, ее бизнес процессов и т.д.;

– Отчеты о финансовых потерях как при восстановлении ресурсов, так и при разглашении информации

– Оценка рисков и угроз для защищаемой системы и поиск ее уязвимостей раз в квартал;

– Составление рекомендуемых контрмер для устранения и уменьшения рисков.

– Рекомендации для данных параметров:

– Соблюдения правил по хранению средств: не использовать личные съемные носители, рабочие съемные устройства должны выдаваться и записываться в журнал;

– Наличие дубляжа информации, который будет храниться в сейфе или у руководителя;

– Разграничения прав доступа к различному виду информации хранящийся на сервере и использовании и хранении криптографических ключей;

– Блокировка системы по кодовому слову или словосочетанию;

– Дубляж криптографических ключей сотрудниками, имеющими на это доступ,

– Создать систему для постоянного резервного хранения данных с постоянным их обновлением и защитой;

– Создание журнала действий администратора и пользователей;

– Присвоение номенклатурного номера всем устройствам на предприятии;

– Использование DLP систем для контроля подключаемых устройств;

– Журнал учета, утилизации устройств;

– Прописанные методы и правила утилизации устаревших устройств.

2) Политика безопасности - выходными данными будут являться:

– Составление отчетов о угрозах, уровнях безопасности и мерах их противодействия;

– Составление отчета об уязвимостях, влияющих на актив. Меры по их устранению и снижению, принятию решения;

– Составление рекомендация по приоритетности действия по защите и увеличению безопасности;

– Постоянный анализ, контроль и разработка стратегий по обеспечению безопасности системы используемое для оценок эффективности стабильного функционирования менеджмента информационной безопасности, с рекомендациями к увеличению и устранению информационная безопасность;

– Составление рекомендаций по улучшению и проведению процедур и мер управления, контроля и систематизации влияющих на защиту информационной безопасности;

– Составление рекомендаций и инструкций для работы в направлении реализации этапов достижения управления рисками и активами в ИТ сфере;

– Контроль за соблюдением политики безопасности, нормативными требования, и мер прописанных для данного предприятия.

Рекомендации для данных параметров:

– Разработка политики безопасности предприятия, ответственных за контролем выполнения мер и средств, пописанных в ней;

– Разработка стратегии для постоянного выполнения, контроля, увеличения действий по повышению защищенности предприятия;

– Назначение ответственных лиц за исполнением политики безопасности предприятия;

– Разработка руководящими лицами целей, задач и принципов информационной безопасности в зависимости от стратегии и целей предприятия;

– Проведение мероприятий по повышению грамотности и переподготовки сотрудников в сфере информационной безопасности;

– Установление и доведение до рабочих методов наказаний при нарушении политики информационной безопасности;

– Установление обязанностей каждого сотрудника и методы информирования об инцидентах безопасности вышестоящему руководству;

– Установление и доведение до рабочих определенных мер, требований, правил безопасности во время работы и действий, возникших при различного рода инцидентах.

– 4) Удаленное оборудование - выходными данными будут являться:

– Анализ, контроль и идентификация всех возможных инцидентов, угроз, уязвимостей;

– Ведения базы выявленных инцидентов, угроз, уязвимостей за определенный период времени;

– Оценка последствий, которые были выявлены при ведении базы выявленных инцидентов, угроз, уязвимостей за определенный период времени;

– Анализ рисков и выделение их основных недопустимых рисков, для дальнейшего принятия решений по их уменьшению и устранению;

– Контроль физической защиты систем;

– Составление журналов, отчетов, диаграмм.

Рекомендации для данных параметров:

– Составление базы и постоянное ее обновление средств любой вычислительной техники, которая будет использоваться персоналом при удаленной работе;

– Запрет на использование личных средств вычислительной техники и мобильных телефонов для организации работы;

– Распределение прав и доступов к данным хранящихся в базе предприятия во время работы, копирования, редактирования, обмена информацией и т.д.;

– Определение удаленных средств вычислительной техники по MAC адресам, к которым будет предоставляться доступ при удаленной работе;

– Назначение ответственного за контролем, предоставлением доступов и анализом выполнения работы;

– Внесение пунктов во внутренние акты предприятия по предоставлению доступа определенным сотрудникам с указанием их ФИО, должности, к каким данным имеют доступ и на какой период времени;

– Ознакомление рабочих под подпись о предоставлении им доступа, всей информации и модификации, которые будут им предоставлены под подпись;

– Разработка, фиксирование в нормативном акте предприятия и доведение под подпись сотрудников об ответственности и наказании при разглашении, умышленном «сливе», порче и др. вида модификации информации и оборудования;

– Организация защищенного удаленного доступа средств вычислительной техники к серверу предприятия;

– Применение средств криптографии для защиты информации;

– Запрет на самостоятельную установку программного обеспечения на удаленные средства вычислительной техники, работа на несертифицированном оборудовании;

– Сформировать перечень возможных средств, программ, которыми можно пользоваться и устанавливать на средства вычислительной техники предприятия и удаленные сервера;

– Назначение ответственного лица за анализом, мониторингом и быстрым и своевременным реагирование за возможными инцидентами, уязвимостями и рисками, возникающими при постоянной работе как средств вычислительной техники, так и сотрудников, работающих удаленно.

5) Изменение и модификация данных - выходными данными будут являться:

– Выявление возможных нежелательных инцидентов, возможных угроз и уязвимостей;

– Выявление вероятности реализации данных угроз;

– Отчет по ущербу от внедрения существующих угроз;

– Формирование отчета о системе на предприятии в целом;

– Формирование отчета о уровнях безопасности, угрозах и возможных мерах для их противодействия;

– Формирование отчета о поведении аудита безопасности;

– Формирования отчета о недопустимых рисках предприятия и возможных мерах воздействия на них;

– Проведение анализа и оценки уровней возможных рисков для используемой информационной системы;

– Формирование отчета по конкретному подобранному обоснованному выбору мер, а также средств защиты от них;

– Определение вероятности и возможной реализации размера ущерба предприятия при определенных рисках, влияющих на систему в целом;

– Отчет о выборе возможных, действующих контрмерах;

– Проведение анализа на соответствие информационной системы требованиям существующих международных стандартов;

– Провести анализ и просчитать возможный ожидаемый ущерб и его вероятностью, оценки приемлемости существующих рисков и шкале необходимости их предотвращения;

– Реализация принятого, обговоренного плана внедрения контрмер с оценкой эффективности от их использования;

– Внедрение в существующую систему новых мер, обязательно сопоставив, проанализировав с уже существующими мерами, механизмов безопасности с расчетом выгоды для предприятия или бизнеса от их внедрения.

Рекомендации для данных параметров:

– Строгий регламент по доступу к информации лиц, отвечающих за работу с ней;

– Недопущение несанкционированного доступа к информации, кражи и передачи ее лицам, которые не имеют право доступа к ней;

– Разработка журналов соответствия возможности доступа к информации в зависимости от должности и форме допуска;

– Разработка методов для постоянного анализа, отслеживания, а также обнаружения фактов неблагоприятных последствий возможных нарушений и доступа к информации;

– Блокировка и применения мер защиты от воздействия на технические средства обработки информации, в результате чего она может быть заблокирована, украдена, изменена или повреждена;

– Разработка мер за постоянным контролем и своевременным применением мер по обеспечению уровня защищенности обрабатываемой информации;

– Установление мест и средств для хранения ценной, защищаемой информации;

– Создание рекомендаций и мер по дублированию циркулирующей информации на предприятии, для высокого уровня ее защищенности;

– Установить для каждого вида ценной информации сроки ее хранения и периодичность дублирования;

– Дублирование информации производить согласно ее защищенности, способам и методам ее хранения, и мерам, прописанным в политике безопасности предприятия;

– Для доступа к информации у пользователей должен быть разработан сложный, уникальный пароль.

– Контроль доступа - выходными данными будут являться:

– Составление отчетов о используемой системе и организации в целом;

– Составление отчета о существующем состоянии безопасности и его уровень;

– Составление отчета об существующих возможных угрозах и их возможных мерах противодействия;

– Составление финансового отчета о ценнике ресурсов, которые подлежат защите;

– Составление отчета о возможных предполагаемых финансовых потерях при реализации угроз;

– Отчет об физической защите защищаемой информационной системе;

– Выявление, постоянное отслеживание и проработка с основными постоянно повторяющимися рисками;

– Создание перечня рекомендаций по каждому направлению и с выстроенными приоритетными действиями;

– Рекомендации по уменьшению или устранению риска;

– Проведение постоянного аудита об применяемых методах и средствах для снижения ожидаемых потерь;

– Фиксирование в специальных журналах предприятия итогов, как промежуточных, так и основных;

– Обязательное документирование возможных рисков информационной безопасности для разных областей;

– Проработка и генерация различных вариантов мер противодействия к найденным рискам в зависимости от их уровня;

– Внедрение ноу-хау для используемой системы в области безопасности и защиты;

– Сопоставление старых и новых механизмов работы и дальнейшая реализация в зависимости от положительного результата;

– Просчет растрат на внедрение новых мер анализа, аудита, защиты и сопоставление их с выгодой для защищаемой системы;

– Сопоставление принимаемых мер с нормативными актами и стандартами;

– Создания комплекса средств защиты.

Рекомендации для данных параметров:

– Разработать комплекс мер по защите информации, который будет защищен от несанкционированного входа;

– Установить контроль доступа для пользователей разных уровней, к разной информации;

– Установить условия применения сложных паролей, которые должны содержать различные символы, буквы верхней и нижней табуляции, длина символов должна быть не менее восьми;

– Установить двухфакторную аутентификацию для входа в систему;

– Необходимо чтобы комплекс средств защиты проверял подлинность идентификации и аутентификации;

– Установить защиту от возможности внедрения злоумышленником управляемой программной закладкой;

– Использовать специальные средства и меры по разграничению доступа к базам данных и информации предприятия, а также к данным хранящимся на сервере;

– Установить средства ограничения физического доступа с помощью аппаратных средств защиты информации;

– Установить средства защиты от НСД по корпоративной сети и сети интернет;

– Установить электронный замок, для защиты от внешних воздействий;

– Использовать проверенные, лицензированные программы для разграничения доступа.

Вывод

Не зависимо от того, будет ли угроза преднамеренная или непреднамеренная, программная ли непрограммная они будут дестабилизировать работу предприятия, что приведет не только к потере репутации, нестабильным доходам, но и самое главное к финансовым потерям или даже банкротству предприятия. Поэтому очень важно, чтоб каждое предприятие постоянно и своевременно разрабатывала списки угроз, проводила их постоянный анализ и принимала конкретные, взвешенные, проработанные решения на их уменьшение и ликвидацию. Желательно чтоб была выстроена система постоянного анализа, контроля, оценки и принятия комплексного решения по всем возникающим вопросам, уязвимостям, рискам. Обязательно на предприятии должны быть прописаны все параметры по оценке, принятию, ликвидации и ответственности за риски, касающиеся данного предприятия, необходимо назначить ответственное лицо за данную работу и

принятие решений. Предприятие может использовать стандартные методики анализа и оценки рисков, но наличие ответственного является обязательным условием. Если предприятие большое, то ему необходимо иметь в штате экспертов или договоренность с внешними экспертами на периодическое проведение экспертизы. Периодичность проведение оценки рисков зависит от необходимости этого для предприятия, сферы ее деятельности, но рекомендуется проводить ее постоянно с одним и тем же промежутком времени – лучше всего раз в квартал, но не менее одного раза за год [7].

В разрабатываемой методике реализуется идея совместить всевозможные результаты для расширения и получения большой базы данных для возможности проводить более глубокую оценку рисков информационной безопасности. Очень часто бывает, что руководители могут и не обращать внимание на возможный риск для какого-либо актива, а он очень даже важен в работе данного предприятия. Поэтому была создана база данных, которая будет постоянно дополняться и усовершенствоваться. На данный момент методика будет оценивать около двухсот входных параметров и более ста выходных параметров, что даст возможность тщательно и глубоко проработать все возможные риски для предприятий, снизить их финансовые и другие потери. Так же методика будет содержать расширенные рекомендации для эффективных принятий решений по уменьшению, устранению, управлению рисков информационной безопасности.

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

Список литературы

1. Маслова М.А. Сравнительный анализ методов оценки рисков информационной безопасности, основанных на стандартных и интеллектуальных подходах / М. А. Маслова, Е. Н. Тищенко // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : материалы XIX Международной научно-практической конференции, Ростов-на-Дону, 28–29 октября 2019 г. Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2019. С. 211-215.

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

3. 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.

4. Баранова Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии исо/мэк 27000-27005 / Е. К. Баранова, А. С. Забродоцкий // Образовательные ресурсы и технологии. 2015. № 3(11). С. 73-80.

5. Коротнев К. Методики управления рисками информационной безопасности и их оценки (часть 1) URL: https://safe-surf.ru/specialists/article/5193/587932/ (дата обращения: 10.10.2022).

6. Пугин В.В. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В.В. Пугин, О.Ю. Губарева // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 6. С. 54-57.

7. Сердечный А.Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT3 в распределенных компьютерных системах / А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина // Информация и безопасность: 2021. Т. 24. Вып. 1. С. 35-46.

Севастопольский государственный университет
Sevastopol State University

Ростовский государственный экономический университет (РИНХ)
Rostov State University of Economics (RINH)

Поступила в редакцию 15.10.2022

Информация об авторе

Маслова Мария Александровна – старший преподаватель кафедры “Информационная безопасность”, Севастопольский государственный университет; младший научный сотрудник, Ростовский государственный экономический университет (РИНХ), e-mail: mashechka-81@mail.ru

SCIENTIFIC AND METHODOLOGICAL RECOMMENDATIONS FOR REGULATION OF INFORMATION SECURITY BREACH RISKS

M.A. Maslova

The article deals with scientific and methodological recommendations regarding the regulation of information security risks. The study contains a generalization of works [1 - 3] on the analysis and management of risks associated with information security. A modification of the Delphi methodology [2] is proposed, implemented and studied in the form of a software prototype. The analysis of the convergence of the results of the proposed methodology is compared with the data and methods: MOF, MSAT, CRAMM, Risk IT, GRIF, OCTAVE, FRAP, CORAS, STO BR IBBS, Risk Watch [4 - 6]. The methodology involves the creation of an extended database of parameters from the above methods with the possibility of its subsequent modification and addition, as well as with recommendations at the output for making effective management decisions, reducing and eliminating information security risks to minimize enterprise losses.

Keywords: information security risks, vulnerabilities, information security risk reduction, recommendations, methods.

Submitted 15.10.2022

Information about the author

Maria A. Maslova – Senior Lecturer of the Department of Information Security, Sevastopol State University; junior researcher Rostov State University of Economics (RINH), e-mail: mashechka-81@mail.ru