DOI 10.36622/VSTU.2022.25.2.006
УДК 004.02 : 004.05

ИНСТРУМЕНТАЛЬНЫЙ ПОДХОД К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. Маслова

Оценка рисков в информационной безопасности, как и в любой области является непрерывным процессом, который необходимо постоянно мониторить, видоизменять, усовершенствовать, так как быстро растущий и постоянно видоизменяющийся информационный поток, появляющиеся новые негативные факторы, а также внутренние и внешние контексты с новыми угрозами могут внести большие потери для предприятий. В условиях постоянных изменений в экономической сфере, необходимо своевременно реагировать на появляющиеся негативные тенденции и оперативно принимать соответствующие меры по их исправлению, т.е. управлять возможными рисками в данной области [1]. Необходимо создавать новые программы, которые будут соответствовать современным требованиям, законодательной базе и быть гибкими к постоянным изменениям во времени и новым появляющимся факторам, рискам и уязвимостям. Также они должны быстро и легко видоизменяться и иметь редактируемую базу данных. В данной статье будет рассмотрена значимость удаленной работы, статистика и приведено описание одного из блоков разрабатывающейся программы для оценки рисков информационной безопасности, которая содержит большую базу входных и выходных DataSet существующих методик.

Ключевые слова: информационная безопасность, риски, выходные данные, DataSet, удаленная работа.

Введение

Информация постоянно видоизменяется и появляются различные факторы, которые кардинально меняют действия, применяемые к ее защите. Так с недавних пор одной из таких факторов стала удаленная работа людей и даже целых компаний и корпораций, следовательно, стала острая необходимость создавать не только другое направление работы и менять его структуру, но и создавать дополнительную защиту от новых рисков, угроз и уязвимостей.

Определение рисков на предприятиях является важнейшей задачей, которая позволяет не только сэкономить деньги от потерь, принять своевременные меры для устранения или уменьшения влияния негативных факторов, но и определить критические факторы, которые несут негативное влияние на все бизнес-процессы предприятия. Поэтому очень важно проводить постоянный контроль и анализ, а также определять риски для выявления утечек информации с корпоративных сетей предприятия.

Необходимо так же внедрять на предприятия новые стандарты для обеспечения конфиденциальности, целостности и доступности информации, которые будут соответствовать всем нормам и требованиям законодательной базы государства, защищать от краж, неправомерного использования финансовых средств, персональных данных людей и киберпреступлений. Необходимо создавать комплексную систему защиты всей информации от: потерь, краж, утечек, фальсификаций, вторжений, видоизменению, и различных модификаций.

За последние годы, появились дополнительные угрозы и уязвимости, связанные с переходом многих предприятий и компаний на удаленную работу. Удаленная работа стала неотъемлемой частью работы любой структуры, а на некоторых предприятиях прижилась и стала практически полной его частью рабочего процесса, так как пандемия дала старт новым виткам развития общества как в цифровой, экономической сфере, так и в сфере практически полной обработки и защиты

информации от различных угроз, компьютерных атак и различных новых факторов, появившихся в данный период.

В период COVID-19 многие компании, которые никогда не применяли данную практику удаленной работы научились сначала внедрять ее понемногу, а позже уже и применили в постоянной работе. Что раньше казалось многим не реально, то сейчас стало вполне хорошей дополнительной практикой в работе начиная с весны 2019 года [2].

В США удаленная работа начала свое развитие раньше и еще до начала пандемии ее развитие росло. По статистике в 2015 году работающих удаленно в США было 3,9 млн. чел., в уже в 2020 году – 4,7 млн. чел. и составляло больше половины сотрудников – 56,8 % (Upwork, 2020) (рис. 1).

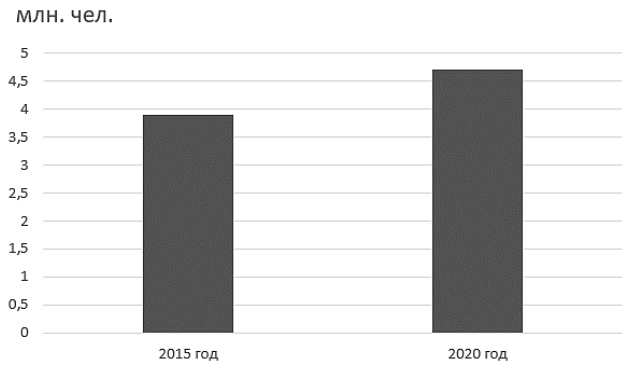

Рис. 1. Рост удаленной работы в США с 2015г. по 2020 г.

Такой формат работы стал набирать популярность из-за определенных положительных факторов: экономия времени на поездки до рабочего места, возможность работать женщинам с маленькими детьми без больничного, больше времени для семьи, гибкий график работы, быстрота и мобильность, больше времени для работы и т.д.

В России и по всему миру также удаленная работа стала более часто встречаться, а из-за пандемии она стала необходимой мерой работы.

За последние два года изменилось отношение в положительную сторону к удаленной работе, если до COVID-19 удаленно работали только 12,3%, то к 2025 году ожидается рост удаленной работы до 22,9% (рис. 2). Еще в феврале 2020 г. 19,5 млн. чел. работали удаленно до 100% времени, то к 2025 году ожидается рост данного фактора до 36,2 млн. чел - это больше чем в половину возрастет число работающий людей полностью в домашних условиях [3].

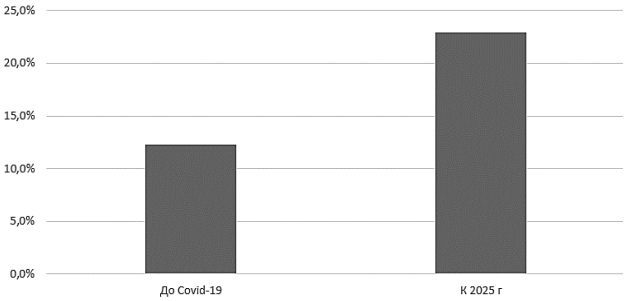

Рис. 2. Рост удаленной работы в мире с 2018г. по 2025г.

Но всегда есть и другая сторона вопроса. Не все отрасли готовы работать удаленно. Если, например, работники сферы финансов, искусства, страхования, технологий, программирования - готовы работать удаленно, то сфера торговли, строительная, образования, медицинская, торговые представители, спорт и некоторые сетевые компании не видят перспектив и улучшения переходя на удаленную работу. Некоторые сферы жизнедеятельности смогут работать в смешанном формате, но много сфер просто не предназначены для этого. Да и большинство людей так же не в восторге от постоянной работы в удаленном формате, так как живое общение пока не может заменить даже самый продвинутый искусственный интеллект.

Например, для больших корпораций и предприятий – это выгодно, т.к. идет снижение огромных расходов на аренду помещений, сокращение работников, счета за коммунальные услуги, уборке помещений, уменьшению использования бумажных вариантов документов, оплаты растрат на проезд сотрудникам (если это предусмотрено), уменьшение зон кафе и мини баров на территории предприятий, и других расходных материалов при обычном очном формате работы.

По приведенным статистическим данным в США при удаленной работе работодатели будут экономить до 30 миллионов долларов (Legal Job Site, 2020) [3].

Но при организации удаленной работы необходимо помнить о защите себя и своих данных и, следовательно, необходимо вкладывать немалые деньги в такие направления, как защита от угроз, утечек информации, атак, т.к. с каждым годом количество атак и утечек растет все больше и их разновидности также видоизменяются.

В период удаленной работы атаки, мошеннические звонки и предлагаемые услуги стали еще больше развиваться и увеличиваться, так как они стали практически не контролируемы, а многие люди были не готовы и грамотно не подкованы в данной области защиты себя и своих данных. Многие по не знанию, по халатности или не достаточной защите своих рабочих мест с домашних компьютеров слили и потеряли много информации в период удаленной работы или попались на мошеннические услуги и предложения.

Если рассматривать конкретно предприятия, то, например, в 2018 году в основном причинами взломов являлись: внешние хакерские атаки – 24,6%, сбои систем безопасности и внутренние уязвимости – 19,5%, человеческий фактор – 18,7% (по данным приведенным институтом Ponemon) [5].

Поэтому компаниям, предприятиям необходимо обязательно уделять большое внимание защите, с помощью:

– обучения сотрудников основам ИБ,

– тестирования применяемых продуктов на предмет уязвимостей,

– использования надежных антивирусных ПО,

– использования официальных ПО,

– применения многофакторной аутентификации,

– применения строгой политики в отношении хранения паролей,

– использования VPN пользуясь общественными сетями,

– применения шифрования данных на жестких дисках ПК.

Только за 2021 год доля хакерских атак выросла на 3% (по данным экспертов Positive Technologies), но их рост замедлился, т.к. организации, предприятия стали более подготовленными к ним, благодаря уже наработанному опыту вовремя COVID-19. В свою очередь главными хакерскими атаками стали:

– вредоносное ПО – 73% среди всех нападений на компании (в основном - это программы шифровальщики, доля которых составляет 69%);

– компрометация компьютеров, сетевого оборудования, серверов - 87 % (в основном программы вымогатели) по сравнению с предыдущими показателями в 71%,

– получение финансовой выгоды – 59 % по сравнению с предыдущими показателями в 43% (в основном данной атаке были подвержены отрасль промышленности, государственные учреждения и медицинские учреждения) (рис. 3).

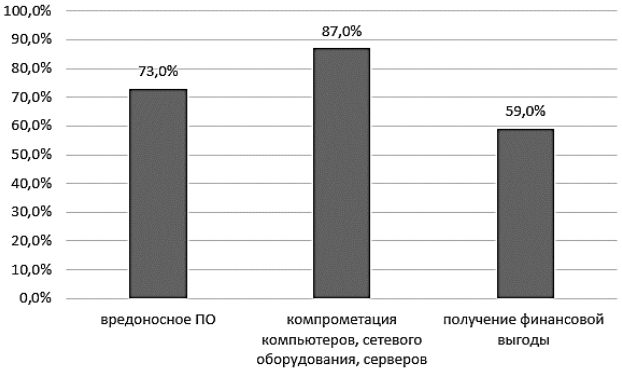

Рис. 3. Хакерские атаки

При этом чаще всего атаки проводят на частных лиц и взлому подлежат личные данные – 78% случаев, в основном это платежные средства, доля которых только за 2021 год выросла более чем в два раза.

В 2021 году статистика немного изменилась и направление хакерских атак стало расти в области криптовалют и составила 47% с января 2021 года по ноябрь 2021 г.

По информации «Лаборатории Касперского» только за первые три квартала 2021 года экспертами было обнаружено 32 новых семейства шифровальщиков и приблизительно около 11000 новых видоизменений вредоносных программ данного типа. Данные атак программ-шифровальщиков на корпоративную компьютерную базу Российской Федерации почти за год составила 14500 раз. В 2020 году

такие хакерские атаки составляли меньше 38% на государственные компании, промышленные предприятия, финансовые учреждения и IT-компании [6].

Очень важно постоянно усовершенствовать программы защиты на устройствах для сохранности своих цифровых активов.

Программы по обнаружению и оценки рисков информационной безопасности не всегда учитывают все активы и направления и тем более не являются хорошо защищены. Любая угроза должна быть идентифицирована и устранена, как бы мелочной она не казалась. Так же необходимо обращать внимание на уязвимости систем управления данными, так как они могут быть связаны с разными активами и принести немалый ущерб предприятию.

Анализ рисков – это трудоемкий и рутинный процесс, поэтому многие консалтинговые компании берут для работы уже готовые разработанные табличные файлы и существующие специальные методики, для того, чтобы облегчить свою работу, уменьшить трудозатраты и финансовую составляющую вопроса. В мире существует множество различных программ, методик и автоматизированных средств для анализа и оценки рисков, например, инструменты и методики анализа рисков:

- AnalyZ,
- BDSS,
- COBRA,
- MELISA,
- PREDICT,
- RANK-IT,
- LRAM & ALRAM,
- Callio Technoloqies: BS7790ISO 17799,
- CONTROL-IT,
- CRAMM, DDIS,
- Digital Security office 2005,
- IST/RAMP,
- LAVA,
- Risiko, riskPAC,
- Security By Analysis, XRM и т.д. [7].

Любое предприятие пытается защитить все свои существующие активы, но иногда на некоторые из них они не обращают внимание, что является большой ошибкой. Так как в информационной безопасности любые активы могут существенно повлиять на работу предприятия, будь то любой процесс, информация, люди, программы, приложения или оборудование и инфраструктура. Поэтому прежде, чем принять какое-то важное решение, необходимо обязательно грамотно выявить и оценить все риски.

На предприятиях создаются отделы информационной безопасности и лица, отвечающие за определение рисков и уязвимостей. Анализ состоит в определение и оценки величины риска состоящий из определенных задач: необходимости определения основных активов и ресурсов информационной системы – определение их важности на предприятии – идентификации существующих угроз и уязвимостей и их осуществление – просчет рисков.

Необходимо определить стоимость ресурса, которую вычисляют в зависимости от величины ущерба, который имеет место при нарушении целостности, доступности и конфиденциальности ресурса, также определяют вероятность угрозы и величину уязвимости, которые между собой связаны формулой:

Величина уязвимости = Вероятность угрозы * Стоимость ресурса.

То есть необходимо создать такую комплексную систему, которая бы позволяла снижать уровень риска нанесения угрозы как можно стремящуюся к минимуму, при этом затраты на внедрение не должны превышать величину ущерба, который нанесен.

Для определения риска, необходимо провести анализ и выделить активы, которые подвержены наибольшей вероятности нанесения вреда, атаке и т.д. и которые необходимо обязательно защитить и про ранжировать их по важности. Так же необходимо рассмотреть из-за чего это происходит и как это можно устранить. То есть при анализе и определении риска необходимо разработать план по обезвреживанию данной угрозы, определить каналы, по которым они были произведены, тип атак, методы защиты от данных атак. После разработать комплексную систему

защиты информации для всего предприятия, учитывая следующие рекомендации:

– рассмотреть и определить угрозы защиты,

– оценить последствия при нанесенной угрозе,

– составить рекомендации, касающиеся методов и средств защиты в соответствии с действующими нормативными требованиями всех нормативных документов,

– рассмотреть совместимость с существующим ПО, а также ее экономическую целесообразность,

– провести оценку эффективности используемого метода и средств защиты.

Благодаря грамотной оценки проведения анализа и определения рисков можно четко сформулировать все действия по устранению рисковых ситуаций и составить грамотные рекомендации для постоянного выполнения. Так как проведение оценки должно быть обязательно системным и постоянным, будут получены объективные оценки всех данных о всей системе в целом. Для качественной работы комплексной системы защиты предприятия необходимо заранее определять и оценивать эффективность мероприятия по защите и тогда потери будут минимальными [8].

Необходимо создать такую программу, которая учитывала бы влияние на все эти аспекты.

То есть необходимо обязательно разрабатывать критерии оценки рисков для информационной безопасности предприятия и учитывать различные аспекты, которые на них влияют. Необходимо оценить все возможные активы, которые могут подлежать рисковым негативным ситуациям, проводить их оценку и составлять, и принимать меры для их устранения. Тогда помимо учета всевозможных активов программа также должна иметь большую базу рекомендаций по решению и устранению рисковых ситуаций.

Для решения данной проблемы была создана программа оценки рисков информационной безопасности, в которой будут учтены всевозможные входные данные (активы) предприятия, которые выбирались из существующих программ оценки рисков информационной безопасности:

– MOF,
– CRAMM,
– Risk IT,
– CORAS,
– ГРИФ,
– MSAT,
– OCTAVE,
– Risk Watch,
– FRAP,
– СТО БР ИББС,
– ISO/IEC 27001 [6, 9].

Для этого проводился анализ и было выделено почти двести входных данных - сходящихся и расходящихся DataSet использующихся в этих методиках и объединены в одну базу, которая доступна экспертам по информационной безопасности реализующим оценку в разработанной программе.

Эксперты и клиенты будут подавать заявку для регистрации и модератор будет отслеживать и подтверждать данные действия.

Для каждого отдельного предприятия эксперты будут выбирать всевозможные активы, которые могут тем или иным способом повлиять на риски данного предприятия, оценивать их по 10 бальной шкале от 0-10 в зависимости от значимости по возрастанию.

Далее экспертам необходимо будет определить выходные DataSet для выбранных активов, которые в свою очередь также выбирались из существующих методик, как сходящиеся и расходящиеся DataSet и заносились в общую базу данных выходных параметров оценки рисков информационной безопасности.

Таблица сходящихся и расходящихся DataSet содержит 62 параметра сходящихся выходных данных и 39 расходящихся выходных данных. Например, сходящиеся выходные данные:

– списки уязвимостей, которые надо устранить в ближайшее время;

– идентификация всех возможных потенциальных нежелательных инцидентов, а также угроз и уязвимостей;

– оценка угрозы в сфере информационной безопасности, поиск и оценка уязвимостей защищаемой системы;

– ожидаемые годовые потери от угроз;

– отчет об организации в целом;

– отчет о результатах аудита безопасности;

– отчет о текущем состоянии уровня безопасности;

– разработка системы показателей рисков;

– ущерб для здоровья персонала;

– ущерб, относящийся разглашением персональных данных отдельных лиц;

– идентификация инфраструктурных уязвимостей;

– формирование подробных отчеты, которые формируются постоянно и проводят сравнение базовых показателей с полученными успехами;

– проверенные, структурированные рекомендации в соответствии с приоритетностью действий для повышения безопасности;

– разработка системы показателей рисков;

– оценка рисков и размер инвестиций в информационных технологиях, а также их объем финансирования ИТ-проектов, основные изменения ИТ-среды, с обязательным мониторингом и тестированием средств управления;

– разработки планов восстановления работоспособности и их регулярного обновления и т.д. [8].

Некоторые из выделенных расходящихся выходных DataSet:

– выявление влияющих проблем, с модификацией решений с последующем внедрением в рабочую среду;

– ИТ-эксплуатация и предоставление услуг - риски, связанные с повседневными операциями и предоставлением услуг ИТ, которые могут вызвать проблемы, неэффективность бизнес-операций организации;

– рекомендации по повышению результативности СМИБ, рекомендации по модификации процедур, а также мер контроля, которые влияют на информационную безопасность, для обеспечения реагирования как на внутренние, так и внешние события, влияющие на СМИБ, включая такие изменения, как требования безопасности; в документах, законах и договорных обязательствах; влияющие на бизнес-требования и бизнес-процессы; влияющие на уровень и/или критерий принятия риска и потребности в различных ресурсах, а также на постоянное улучшение способов оценки результативности мер управления;

– детальное описание инструкций по реализации всех этапов управления рисками, включающих обзор ключевых факторов успеха, типовые перечни ИТ-активов, уязвимостей, угроз, шаблонов документов, которые реализуют процесс управления рисками ИБ;

– рекомендация относящиеся к бизнес-аспектам и принимаемые решения, такие как оценка рисков, инвестиции в информационные технологии и их объем финансирования, а также периодический мониторинг и тестирования всех средств управления.

– потери, связанные с невозможностью выполнения обязательств;

– выбор адекватных контрмер;

– составление плана для внедрения новых контрмер с оценкой эффективности использования;

– использование комбинированного подхода оценки рисков: на входе применение качественного подхода, на выходе количественная оценка;

– для определенной области исследования выявляется, оценивается и составляется документальная часть для рисков ИБ с последующем внедрением процессов управления рисками на все направления организации и т.д. [8].

Так, учитывая всевозможные активы и меры принятия к рисковым ситуациям программа может оценивать большое количество параметров и, следовательно, оценка рисков будет более точной и грамотной. Данная сходимость будет проверяться с помощью автоматического

вычисления вспомогательных параметров и дисперсии и проверяться на сходимость.

Работа программы будет осуществляться с помощью удаленного доступа, что в сложившемся обществе есть нормой и иной раз необходимой мерой, а также дает возможность привлечь разных специалистов независимо от их удаленности от данного предприятия, то необходимо не забывать о возможной степени опасности удаленной работы.

Необходимо обязательно предусмотреть требования к управлению безопасности процессов удаленной работы: политик, программ, измерением процессов и т.д., учитывая все факторы возможного влияния угрозы информации. Так как с развитием удаленной работы участились угрозы утечек данных и их кража, несанкционированный доступ к информационным системам. Необходимо также обратить внимание и постоянно усовершенствовать способы хранения и управления данными в облачных хранилищах, обновлять устаревшие устройства веб-защиты и механизмы удаленного доступа.

Данная программа предполагает постоянное усовершенствование базы данных как входных, так и выходных параметров, постоянной корректировки ее модератором, добавление параметров и мер защиты с появлением новых сценариев угроз и уязвимостей.

Заключение

Можно сделать вывод, что удаленная работа на сегодняшний день является неотъемлемой частью нашего общества, а в некоторых ситуациях, как с COVID-19 ключевым фактором положительной и непрерывной работы предприятий. Поэтому создающийся программный код разрабатывался для дальнейшего его использования полностью с помощью удаленной работы как клиентов, так и экспертов, что позволит оперативно, гибко проводить экспертизы рисков информационной безопасности для предприятий в любой точке мира не зависимо от часового пояса и занятости всех сторон, принимающих решение в данной программе. Программа будет обеспечивать эффективную, выстроенную работу на основе реальных оценок процесса анализа рисков. За счет большой базы данных входных и выходных DataSet она будет достаточно гибкой в работе, ее можно будет просто и быстро редактировать, дополнять видоизменять, модифицировать.

Список литературы

1. Кайтмазов, В.А. Риск и управление риском (риск-менеджмент) в системе экономической безопасности / В.А. Кайтмазов // Вестник московского университета МВД России. Сер. Экономические науки. 2020. № 12. С. 131-137.

2. Сердечный А.Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT3 в распределенных компьютерных системах / А.Л. Сердечный [и др.] // Информационная безопасность: Сб.науч.тр. Воронеж: Изд-во ВГТУ. 2021. Т. 24. ВЫП. 1. С. 35-46.

3. 10 статистических данных об удаленной работе, которые вам нужно знать в 2021 году URL: https://aliexpress.inform.click/10-statisticheskih-dannyh-ob-udalennoj-rabote-kotorye-vam-nuzhno-znat-v-2021-godu (inform.click)/ (дата обращения 10.04.2022).

4. Солдатова, С.С. Экономические последствия пандемии «COVID-19» для России / С.С. Солдатова, К.Р. Пивкина // StudNet. Т. 3. № 2. 2020. С. 260-265.

5. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома. URL: https://vc.ru/services/103616-utechki-dannyh-3332019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma (дата обращения 16.04.2022).

6. 47% хакерских атак в 2021 году пришлись на программы-шифровальщики. URL: http://cchia.ru/47-hakerskih-atak-v-2021-godu-prishlis-na-programmy-shifroval-schiki/ (дата обращения 26.04.2022).

7. Методики управления рисками информационной безопасности и их оценки (часть 2). URL: Https://safe-

surf.ru/specialists/article/5194/587935/ (дата обращения 18.04.2022).

8. Пашков, Н.Н. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии / Н.Н. Пашков, В.Г. Дрозд // Современные научные исследования и инновации. 2020. № 1. URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 06.04.2022).

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

Севастопольский государственный университет
Sevastopol State University

Поступила в редакцию 15.05.2022

Информация об авторе

Маслова Мария Александровна – старший преподаватель кафедры “Информационная безопасность”, Севастопольский государственный университет, e-mail: mashechka-81@mail.ru

INSTRUMENTAL APPROACH TO INFORMATION SECURITY RISK ASSESSMENT

M.A. Maslova

Risk assessment in information security, as in any field, is a continuous process that needs to be constantly monitored, modified, improved, since the rapidly growing and constantly changing information flow, emerging new negative factors, as well as internal and external contexts with new threats can cause great losses for enterprises. In the conditions of constant changes in the economic sphere, it is necessary to respond in a timely manner to emerging negative trends and promptly take appropriate measures to correct them, i.e. to manage possible risks in this area [1]. It is necessary to create new programs that will meet modern requirements, the legislative framework and be flexible to constant changes over time and new emerging factors, risks and vulnerabilities. They should also be modified quickly and easily and have an editable database. This article will consider the importance of remote work, statistics and a description of one of the blocks of the program being developed for assessing information security risks, which contains a large database of input and output datasets of existing techniques.

Key words: information security, risks, input data, output data, DataSet, remote work.

Submitted 15.05.2022

Information about the author

Maria A. Maslova – Senior Lecturer of the Department of Information Security, Sevastopol State University, e-mail: mashechka-81@mail.ru