УДК 004.588

Вестник УрФО № 4(42) / 2021, с. 46–58

Астахова Л.В., Киряев А.И.

DOI: 10.14529/secur210405

ИНТЕГРАЦИЯ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ДОКУМЕНТАМИ И ОСВЕДОМЛЕННОСТЬЮ СОТРУДНИКОВ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО ПРЕДПРИЯТИЯ

В статье определены факторы, влияющие на организацию работы с документированной информацией и управление осведомленностью сотрудников в области информационной безопасности (ИБ) в процессе ее управления на малых и средних предприятиях. К ним относятся требования международных и национальных стандартов управления информационной безопасностью (УИБ) и других нормативных документов; документальный формат проверок состояния организаций ИБ регулирующими органами; недостаточная осведомленность персонала о документально оформленных правилах обеспечения информационной безопасности; недостаточное внимание предприятий к документированию процессов обеспечения ИБ организаций, а также осведомленности сотрудников об ИБ. Особенно низка эффективность работы с документацией по ИБ на малых и средних предприятиях. В процессе анализа мирового потока научной литературы была выявлена необходимость усиления взаимосвязей процессов управления информационной безопасностью, их документирования и автоматизации. Цель исследования - разработать средство оптимизации системы менеджмента информационной безопасностью (СМИБ) организации на основе многофункциональной автоматизированной деятельности с документированной информацией об ИБ путем ее интеграции с управлением осведомленностью персонала об этой документации. Материалы и методы. Для решения проблемы использованы интеграционный подход к процессам построения СМИБ, аналитико-синтетические методы, метод моделирования процессов и программирования. Результаты. В контексте выявленных тенденций и накопленного практического опыта в статье обосновывается необходимость и результат разработки многофункционального программного приложения для организации работы с документацией по управлению

информационной безопасностью малых и средних предприятий. Приложение может выполнять функции создания и обновления; распространения, доступа, поиска и использования; хранения и консервации; управления изменениями; контроля осведомленности сотрудников о документированной системе информационной безопасности организации. Научная новизна заключается в обосновании и реализации интегративного подхода к управлению документацией по ИБ и управлению осведомленностью об ИБ сотрудников организации. Практическая значимость работы заключается в возможности использования разработанного веб-приложения на малых и средних предприятиях для оптимизации процессов защиты информации.

Ключевые слова: *управление информационной безопасностью, документация, осведомленность, интеграция, автоматизация, программное приложение, малые и средние предприятия.*

Astakhova L.V., Kiryaev A.I.

INTEGRATION OF AUTOMATED MANAGEMENT OF DOCUMENTS AND AWARENESS OF EMPLOYEES ABOUT INFORMATION SECURITY OF A SMALL AND MEDIUM ENTERPRISE

The article identifies the factors influencing the organization of work with documented information and the management of the awareness of employees in the field of information security (IS) in the process of its management in small and medium enterprises. These include the requirements of international and national standards for information security management (ISM) and other regulatory documents; the documentary format of inspections of the state of information security organizations by regulatory authorities; insufficient awareness of personnel about the documented rules for ensuring information security; insufficient attention of enterprises to documenting the processes of ensuring information security of organizations, as well as awareness of employees about information security. The efficiency of work with information security documentation is especially low in small and medium-sized enterprises. In the process of analyzing the global flow of scientific literature, the need to strengthen the interconnections of information security management processes, their documentation, and automation was identified. The purpose of the study is to develop a tool for optimizing an organization's information security management system (ISMS) based on multifunctional automated activities with documented information about IS by integrating it with personnel awareness management about this documentation. Materials and methods. To solve the problem, and integrated an approach to the processes of building an ISMS, analytical and synthetic methods, a method of modeling processes and programming were used. Results. In the context of the identified trends and the accumulated practical experience, the article substantiates the need and the result of developing a multifunctional software application for organizing work with documentation on information security management of small and medium-sized enterprises. The

application can perform creation and update functions; distribution, access, search and use; storage and conservation; change management; control of the awareness of employees about the documented information security system of the organization. Scientific novelty lies in the substantiation and implementation of an integrative approach to the management of information security documentation and management of information security awareness of the organization's employees. The practical significance of the work lies in the possibility of using the developed web application in small and medium-sized enterprises to optimize information security processes.

Keywords: *information security management, documentation, awareness, integration, automation, small and medium enterprises.*

1. Введение

Анализ утечек конфиденциальной информации за 9 месяцев 2020 года показал, что в мире было зарегистрировано на 7,4% меньше утечек, чем за аналогичный период прошлого года. Однако в России за тот же период количество утечек увеличилось на 5,6%. Если в мире 52,6% утечек вызваны внешними воздействиями, то в России - в пределах 21%, поскольку более 79% утечек произошли в результате внутренних нарушений. Также в России доля утечек по вине сотрудников вдвое выше, чем в мире - более 72%. [1]. Эти статистические данные свидетельствуют о том, что решение внутри организационных проблем управления информационной безопасностью требует особого внимания как в теоретическом, так и в практическом плане. Необходимы новые подходы к управлению информационной безопасностью организации. Важнейшими направлениями управленческой деятельности в области информационной безопасности являются управление документацией по ИБ и управление осведомленностью персонала об этой документации. Однако эти процессы чаще всего реализуются локально, изолированно друг от друга. Это обусловливает актуальность и цельнастоящегоисследования - разработать средство оптимизации системы менеджмента информационной безопасностью (СМИБ) организации на основе многофункциональной автоматизированной деятельности с документированной информацией об ИБ путем ее интеграции с управлением осведомленностью персонала об этой документации.

2. Вопросы управления документами и осведомленностью об информационной безопасности в теории и практике СМИБ

Управление информационной безопасностью активно изучается в мировой теории и практике, чему способствует стандартизация этой сферы деятельности. Первоначально стандартизация была сосредоточена на технологических аспектах - контроле доступа, сетевой безопасности и т. д. В начале двадцатого века начался процесс выпуска международных оценочных стандартов, определяющих критерии оценки соответствия компьютерных систем требованиям безопасности. Далее стали создаваться документы, в которых внимание сосредоточено исключительно на проблемах СМИБ: построение СМИБ организации, управление рисками, инциденты, аудит ИБ и др. Были разработаны серия международных стандартов ISO / IEC 27000, ISO / IEC TT 33052: 2016, а также библиотека мер контроля из серии стандартов NIST 800 и немецкий стандарт BSI. Наконец, последней тенденцией является разработка стандартов корпоративного управления (управления) информационной безопасностью: O-ISM3 (OpenInformationSecurityMaturity Model); COBIT 19, ISO / IEC 27014-20 и т. д.

Каждый из этих стандартов уделяет внимание управлению документацией по информационной безопасности. Так, согласно стандарта ISO / IEC 27001-2013 [2], эксперты включают в состав документации по ИБ обязательные и необязательные документы и записи. В число обязательных документов они включают: Область действия СМИБ (п. 4.3); Политика и цели информационной безопасности (пункты 5.2 и 6.2); Методология оценки рисков и обработки рисков (п. 6.1.2) и др. [3]. Специалисты также предлагают другие классификации документов, выделяя обязательные (28 документов), рекомендуемые (32 документа) и полезные (15 документов) документы [4].

Большое внимание уделяется контролю документированной информации в практике. Документация должна контролироваться с точки зрения: 1) создания и обновления (идентификации и описания (название, дата,

автор, версия); формата (язык, версия программного обеспечения, графика) и носителя (бумажный, электронный); проверки и утверждения для пригодности и адекватности); 2) распространения, доступа, поиска и использования (информация о распространении (имя получателя, количество копий, местонахождение); контроля доступа, извлечения и использования (уровень доступа, что должно быть доступно, время и продолжительность доступа, используемый метод, срок действия, количество поисков); регулярной проверки предоставленных прав доступа (в том числе новый запрос доступа / поиска, прекращение или отзыв доступа); 3) хранения и консервации (носитель (в сети Интернет, в печатном или электронном виде); прав человека на доступ к хранению документированной информации); 4) контроля изменений (детали модификации (имя человека, дата изменения, журналы истории, номера версий),причины изменений); 5) хранения и порядка утилизации (срок хранения, причины хранения, подробности утилизации (ответственное лицо, дата утилизации, что и почему должно быть удалено) [5, 6]. ISO / IEC TT 33052: 2016 также выделяет группу процессов управления документами и их отношения с группами процессов PRM.

COBIT 2019 усиливает акцент на создании системы управления информационной безопасностью, в задачи которой входят и задачи, связанные с людьми, их компетенциями, навыками икультурой поведения [5]. Представленные задачиможно использовать для подготовки должностных инструкций, программ повышения осведомленности и др. [7].

Особое внимание уделяется документу «Политика информационной безопасности», которая является одним из наиболее важныхформальных документальных средств контроля [8, 9]. Так, была разработана концептуальная основа для создания политики информационной безопасности [10]. В последние годы интерес исследователей прикован к компьютеризированным инструментам, которые поддерживают работу менеджеров по информационной безопасности [9, 11 и др.]. В качестве примера приведем обзор существующих исследований в области управления политикой ИБ, целью которого было изучение соотношения ручной и компьютеризированной поддержки СМИБ и средств их реализации. Авторы пришли к выводу, что существующие исследования сосредоточены в основном на поддержке ручного управления, поэтому разработали программное обеспечение для компьютеризированной поддержки отдельных процессов управления рисками, разработки, соблюдения и мониторинга политики ИБ [12].

В цифровой экономике открываются новые возможности для автоматизации работы с документацией, что немаловажно для сектора информационной безопасности. В условиях цифрового производства должны быть переведены в цифровой формат не только документация, но и методы ее формирования и методологии управления. Автоматизированные системы управления информационной безопасностью решают множество задач, включая обеспечение управления документами. Это позволяет не только улучшить эффективность системы защиты информации, но и выполнить требования большого количества международных и российских стандартов в области информационной безопасности.

Зарубежные специалисты выявили требования к компьютеризированным инструментам и создали программу «TheInformation SecurityGovernanceToolbox (ISGT)». После установления требований безопасности организации, выбора соответствующих мер безопасности и поддерживающих процедур безопасности программа динамически составляет документацию по безопасности, необходимую для обеспечения соблюдения этих мер информационной безопасности. К числу создаваемых документов относятся: корпоративная политика информационной безопасности, краткая и полная версия; политики вторичного уровня в виде различных поддерживающих стандартов компании, которые отражают выявленные меры безопасности; соответствующие процедуры безопасности, связанные с политикой, заявление о применимости. Этот набор документации предлагается пользователю в виде документов Word, которые можно изменять и корректировать в соответствии с конкретными потребностями организации. Программа также хранит копии этих документов, к которым можно получить доступ в любое время, пока не будут разработаны их новые версии [11].

Рассматриваются возможности автоматизации различных видов работ с документацией с использованием программных роботов. Существует понятие «роботизированная автоматизация процессов», и перспективы, связан-

ные с созданием «роботизированных» документов, весьма широки. В настоящее время уже есть опыт роботизации работы с документами, например, с договорами в государственной корпорации «Росатом» на основе решения компании ABBYY [13]. Это позволяет видеть перспективы работы с документацией по ИБ.

В России разработаны и используются в практике продукты для автоматизации работы с документами по ИБ (КИТ-Журнал, АльфаДок). Например, «КИТ-Журнал» облегчает подготовку следующих документов: Список допущенных к работе с ключами СКЗИ / в помещения с ключами СКЗИ; Список лиц, имеющих доступ к содержанию электронного журнала сообщений; Список лиц, допущенных к защищаемой информации; Заявка на предоставление или изменение доступа; Матрица доступа, перечень защищаемых ресурсов и др. Шаблоны документов встроены в программу, но предусмотрена возможность добавления и пользовательских шаблонов документов. Этот функционал позволяет достичь экономии времени за счет мгновенного формирования документов. Программа «АльфаДок» также обеспечивает автоматизированную разработку документации по защите информации и позволяет поддерживать документы в актуальном состоянии в случае изменений в нормативной базе и внутри организационных изменений, таких как кадровые изменения, замена оборудования, программного обеспечения и др.

Повышение осведомленности персонала об ИБ также является актуальной проблемой. Международные стандарты по управлению информационной безопасностью включают не только требования, но и рекомендации по работе ссотрудниками. Особое внимание уделяют обучению сотрудников правилам информационной безопасности и повышению их осведомленности об этих правилах. Серия стандартов ИСО/МЭК 2700 по управлению информационной безопасностью предполагает наличие в организации эффективной программы повышения осведомленности, обучения и подготовки по ИБ, доводящей до сведения всех сотрудников их обязанности по обеспечению ИБ, сформулированные в политиках и стандартах ИБ, и побуждающая их к соответственным действиям. В стандарте ISO/IEC 27001:2013 InformationTechnology — SecurityTechniques — InformationSecurityManagementSystems — Requirements («Информационная технология — Методы и средства обеспечения безопасности — Системы менеджмента ИБ — Требования») в подразделе 7.3. «Осведомленность» (Awareness) приведены требования к сотрудникам организации: они должны быть осведомлены о политике ИБ; своем вкладе в обеспечение эффективности системы менеджмента ИБ, включая выгоды от улучшения функционирования ИБ; последствиях несоблюдения требований системы менеджмента ИБ [2]. Рекомендации по осведомленности, обучению и тренингам в области информационной безопасности, а также перечень мероприятий на разных этапах занятости сотрудника (в период трудоустройства, занятости и увольнения) содержит стандарт ISO/IEC 27002:2013 InformationTechnology — SecurityTechniques — CodeofPracticeforInformationSecurityControls («Информационная технология. Методы и средства обеспечения безопасности. Свод правил по мерам и средствам контроля и управления информационной безопасностью») [14]. Рекомендации по разработке программы информирования, обучения информационной безопасности представлены в п.7.3. «Awareness» стандарта ISO/IEC 27003:2017 [15].

Повышению осведомленности посвящены рекомендации и руководства. Документ «InformationSecurityAwarenessinFinancialOrganisations» (ENISA, 2008) содержит рекомендации по повышению осведомленности по вопросам ИБ в финансовых организациях [16]. «Модель зрелости осведомленности по вопросам безопасности» (SecurityAwareness Maturity Model) (Европейская научно-образовательная организация «The SANS Institute», 2011) дает возможность организациям определить, на каком этапе находится их программа повышения осведомленности о безопасности в настоящее время и в каком направлении следует двигаться в дальнейшем [17]. В ответ на быстрые темпы цифровизации специалисты сформулировалии изучают концепцию цифровой среды как киберпространства, концепции культуры кибербезопасности, цифровой культуры безопасности и т. д. Эти концепции должны лежать в основе культура информационной безопасности любой организации. Агентство Европейского Союза по сетевой и информационной безопасности (ENISA) приложило большие усилия для развития этих концепций. В 2017 году опубликован документ «CyberSecurityCultureinorganisations», в котором описываются рекомендации

и передовой опыт по созданию программ повышения культуры кибербезопасности, восемь этапов и пошаговые инструкции их реализации [18].

Вначале 20 века появилось важное направление в науке - культурология информационной безопасности. Широта и глубина исследований в этой области подтверждается масштабными обзорами публикаций по данной теме:с 2000 по 2013 год [19]; с 2003 по 2016 год [20]; с 2000 г.до 2017 г. [21] и др.

В России также уделяется определенное (хотя и меньшее) внимание сотруднику организации в контексте информационной безопасности. Развитие нормативной правовой базы (Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных», приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды», приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечениюбезопасности значимых объектов критической информационной инфраструктуры Российской Федерации», российские стандарты по управлению информационной безопасностью, стандарты Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации и другие нормативные правовые и методические документы Российской Федерации) способствовало развитию рынка услуг по повышению осведомленности об информационной безопасности (KasperskySecurityAwareness (Лаборатория Касперского), PhishmanИнформационный центр (Phishman), Антифишинг (Антифишинг) Company), SecurityAwarenessPlatform (UBS), SyssoftSecurityAwareness (SyssoftCompany), DeteactAwareness(DeteAct) и т. д.). Однако, несмотря на это, серьезные проблемыповышенияосведомленности персоналаоб информационной безопасности и культуры их информационной безопасности остаются [22].

В связи с изложенным мы считаем, что одним из важных факторовналичия этой проблемы - отсутствие взаимосвязимежду процессами управления документами иосведомленностью. В существующих исследованиях не уделялось особого вниманиявзаимодействию между различными этапами менеджмента ИБ, таких исследований немного. Так, исходя из требований стандарта [23], автор обосновывает связьмежду всеми группами процессов PRM и группойпроцессы управления документами [24].Тем не менее большинство экспертов приходят к выводу, что дальнейшие исследования должныуделять больше внимания взаимодействию между этапами управления политикой информационной безопасности, развивать дополнительные исследования для разработки компьютеризированной поддержки управления ИБ, изучать степень, до которой компьютеризированная поддержка может улучшить интеграцию этапов управления ИБ и упростить управление процессами [8, 12]. Полагаем, что это в полной мере относится и к взаимосвязям между группами процессов, входящих в «Общие интегрированные процессы управления» - Управление документацией (COM 02) и Управление человеческими ресурсами (COM 03).

Необходимость интеграции процессов управления документацией и осведомленностью сотрудников обусловлена еще одним фактором - документационный формат контроля ИБ и УИБ.

Приступая к конкретной проверке, относящейся к информационной безопасности, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, обычно начинают со сбора предварительной информации из различных источников. Это результаты предыдущих проверок, тестирований и оценок, частично или полностью относящихся к текущей области проверки и так или иначе выполненных аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью (например, предварительные тесты безопасности, проведенные специалистами по обеспечению информационной безопасности, могут дать обширные знания по безопасности основных прикладных систем); сведения о соответствующих инцидентах информационной безопасности, ситуациях, близких к инцидентам, вопросах поддержки и изменениях, полученные от службы технической поддержки ИТ, из процессов менеджмента изменений ИТ, процессов менеджмента инцидентов ИТ и из аналогичных источников;

Согласно ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011 «Информационная технология

(ИТ). Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью», к методам проверки, наряду с опросом и тестированием, относится изучение (п. 7.2.). Объекты проверки обычно включают в себя спецификации - документы, устанавливающие требования (см. ГОСТ ИСО 9000-2011, пункт 3.7.3). К ним относятся политики, планы, процедуры, требования к системам, технические инструкции и руководства пользователя/администратора и др. Кроме того, в приложение В включен раздел В1 Кадровые ресурсы и безопасность для проверки мер и средств контроля и управления ИБ, связанной с сотрудниками организации (чувствует ли персонал себя ответственным и/или подотчетным за свои действия; является ли персонал заслуживающим доверия, чтобы обращаться с чувствительной информацией и системами, которые могут подвергать опасности продолжительность существования организации; является ли персонал таким, которому можно полностью доверять; как определяется и измеряется доверие и др.) [25].

Особенно остро стоит проблема интеграции процессов УИБ на малых и средних предприятиях, работающих в условиях ограниченных финансовых, кадровых, временных и др.ресурсов и, следовательно, уделяющих недостаточное внимание этой проблеме. Эксперты единодушны в том, что объем документированной информации для СМИБ может отличаться от одной организации к другой из-заразмера организации и вида ее деятельности; процессов, продуктов и услуг; сложности процессов и их взаимодействия; компетентности сотрудников [3, 4]. Поэтому обнаружено [11], что многие малые и средние предприятия не придерживаются принципов управления безопасностью, в основном, из-за ограниченных ресурсов и опыта. Это особенно верно для тех принципов, которые используются при разработке политик информационной безопасности и мониторинге их соблюдения. Исследования показывают, что эта проблема существует во всем мире и оказывает особенно большое влияние на малый и средний бизнес, которому в настоящее время требуется не теоретическая, а в большей степени практическая помощь в виде процессов, процедур и инструментов, которые они могут использовать в реальных условиях.

3. Программное решение для интеграции управления документами и осведомленностью об ИБ

Чтобы решить обоснованную выше проблему, мы разработали прототип веб-приложения для интегрированного управления документацией по информационной безопасностии осведомленностью сотрудников о ней. Веб-приложение предназначено для модернизации системы управления информационной безопасностью в малом и среднем бизнесе.

Веб-приложение разработано на Python с использованием Фреймворков Django, Bootstrap (интерфейс). SQLite использовался в качестве базы данных, которая используется Django по умолчанию. Python – это универсальный язык программирования высокого уровня, ориентированный на повышение производительности труда разработчиков и читаемость кода. Django – это бесплатный фреймворк для веб-приложений Python, который использует шаблон проектирования MVC. SQLite – это встраиваемая кроссплатформа баз данных, поддерживающая достаточно полный набор SQL команд. К достоинствам Django можно отнести безопасность, масштабируемость, универсальность, скорость развития и др.

Веб-приложение можно разделить на две части: административная панель и панель пользователя. Административная панель позволяет управлять настройками сети (рис.1).

Информация о пользователе выглядит на панели администратора следующим образом (рис.2).

Пользовательская панель предназначена для просмотра документации по информационной безопасности и информации о ней. Панель авторизации изображена на рис.3.

После авторизации открывается панель пользователя (рис. 4), позволяющая работать с документацией по информационной безопасности и проходить тестирование на осведомленность о них.

Для работы программы администратор вводит в базу данных полный пакет документов по информационной безопасности предприятия и заполняет информацию о них. В содержание информации о каждом документе входит: Тип документа; Имя; Дата утверждения; Период действия; Утверждено; Ответственный; Описание; Список ознакомления.

Администратор может редактировать документ (рис.5).

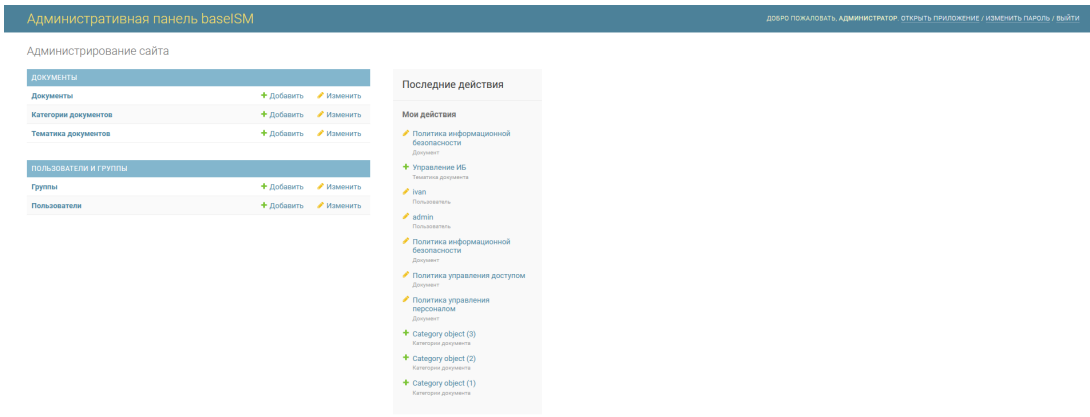

Рис. 1. Панель администратора

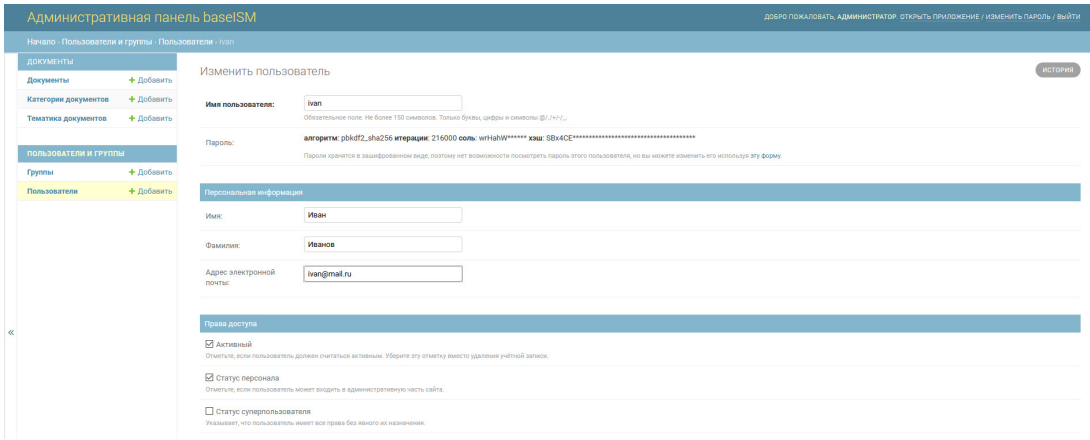

Рис. 2. Информация о пользователе на административной панели

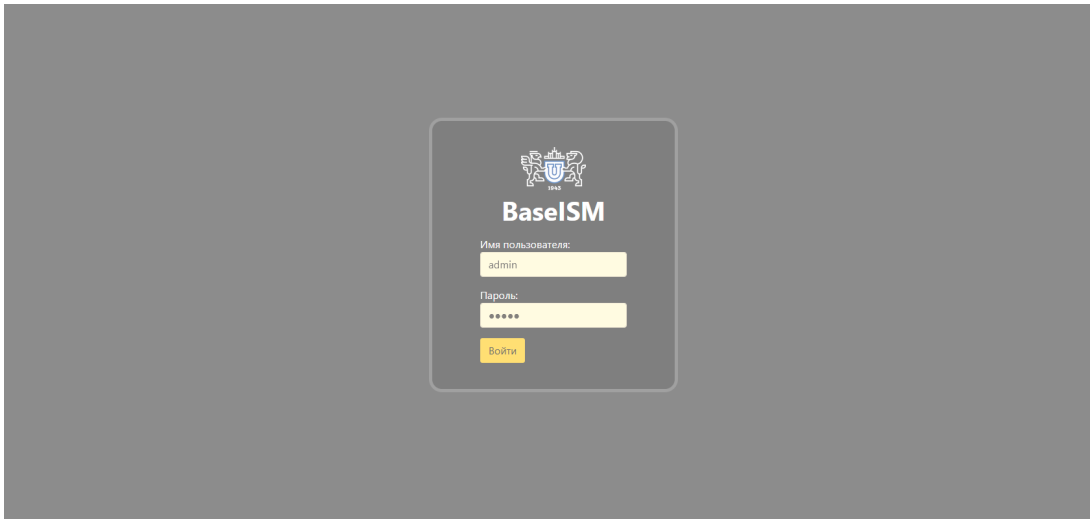

Рис. 3. Панель авторизации пользователя

Сотрудник может работать с документом при наличии права доступа, изучать его, после чего должен сделать отметку об ознакомлении в поле «Ознакомлен» (рис.6).

Администратор следит за процессом ознакомления сотрудников с документацией (рис.6) и процессом тестирования в рамках повышения осведомленности персонала об информационной безопасности (рис.7). Анализ и интерпретация результатов тестирова-

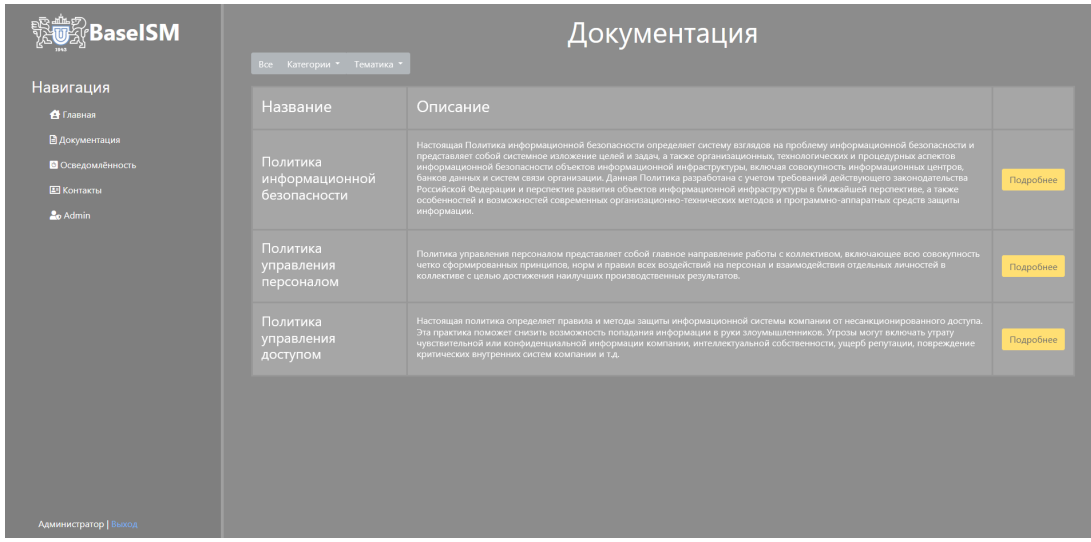

Рис. 4. Панель пользователя

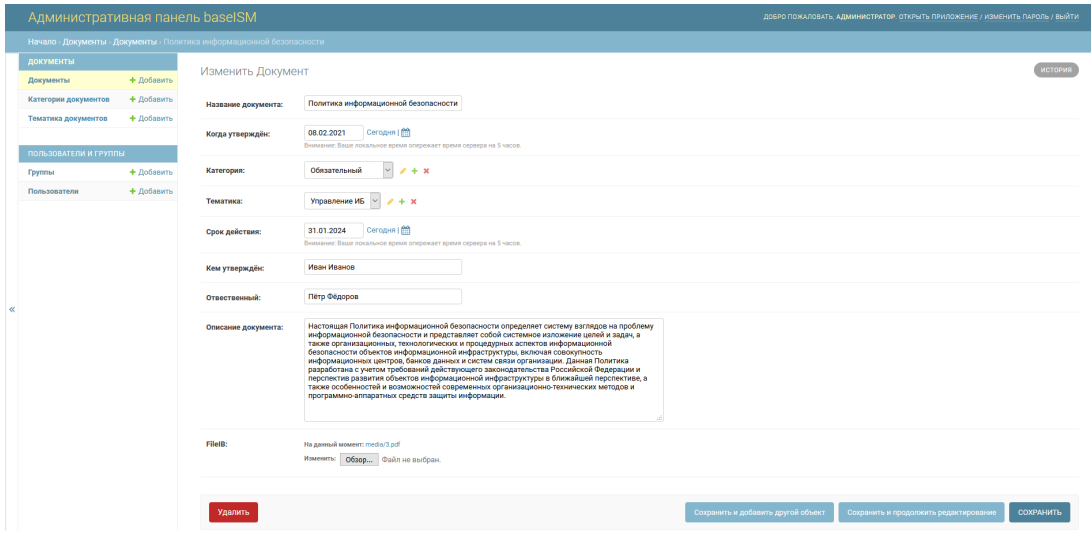

Рис. 5. Панель редактирования информации о документе

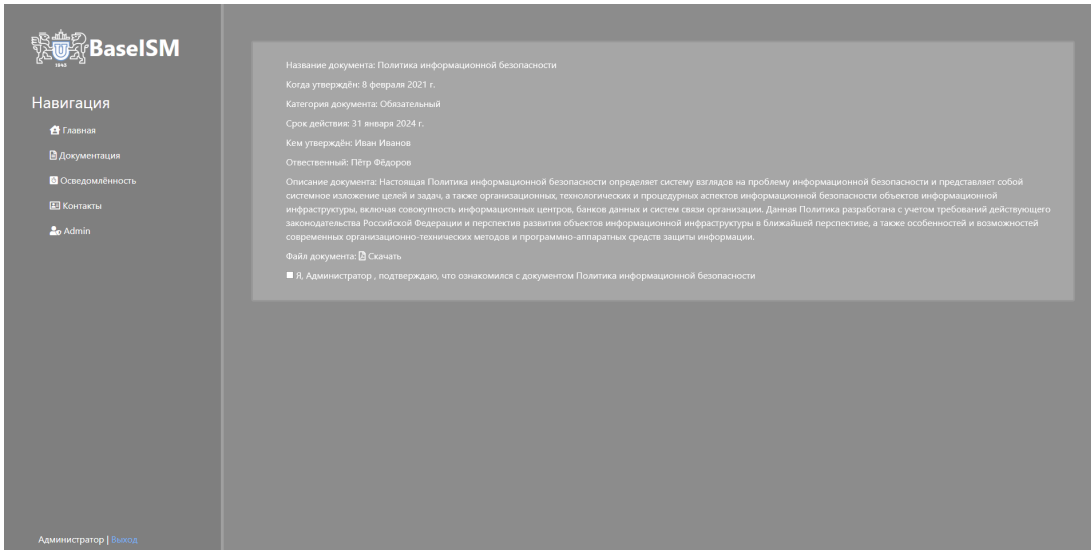

Рис. 6. Панель работы пользователя с документом

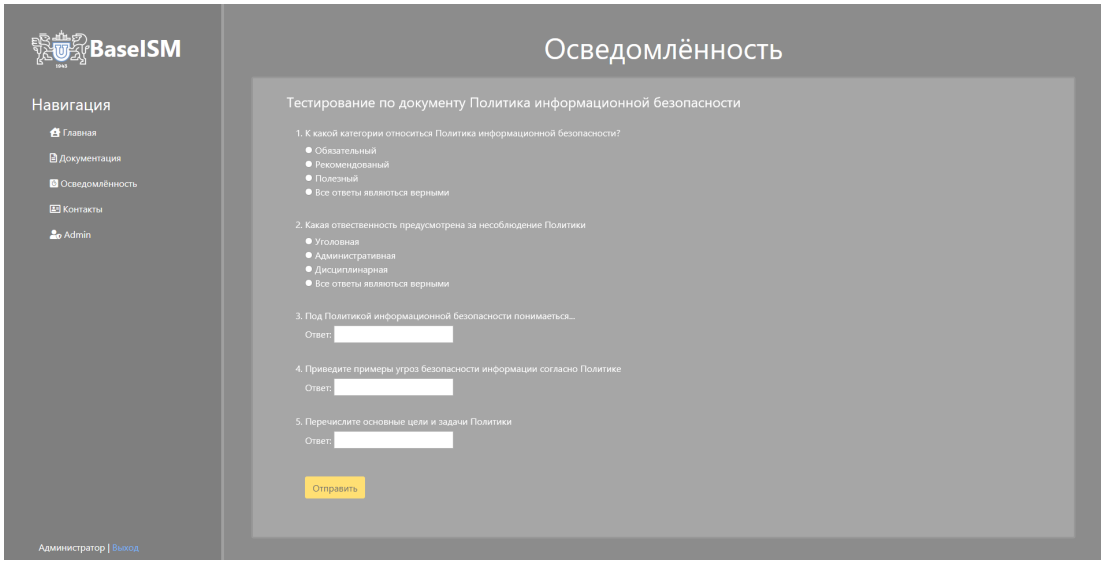

Рис. 7. Панель тестирования сотрудника на знание документа

ния осуществляется только в контексте общей системы управления информационной безопасностью каждой конкретной организации, что является предметом отдельной публикации.

Функциональность представленного веб-приложения не ограничена. В разработке находятся функции управления активами, управления инцидентами информационной безопасности, управления уязвимостями, управления аудитами.

4. Заключение

Анализ публикаций показал проблему отсутствия взаимосвязи между процессами управления информационной безопасностью в организациях. Для решения этой проблемы мы разработали многофункциональный веб-инструмент для интеграции двух процессов управления – управления документами и управления осведомленностью сотрудников о документированных правилах информационной безопасности организации. Продукт может помочь минимизировать затраты на ресурсы для реализации СМИБ-процедур. Научная новизна исследования заключается в обосновании интегративного подхода к управлению системой документации в области ИБ и управлению осведомленностью сотрудников организации об этой системе. Практическое значение работы заключается в возможности использования разработанного веб-приложения на малых и средних предприятиях для оптимизации процессов обеспечения информационной безопасности.

Литература

1. InfoWatch. Restricted Information Leaks: 9 Months 2020 Report. - Available at: https://www.infowatch.ru/analytics/reports/30708 (accessed 31.03.2021).

2. ISO/IEC 27001-2013 Information technology — Security techniques — Information security management systems — Requirements. - Available at: https://www.iso.org/standard/54534.html(датаобращения:19.05.2021).

3. Biswas P. ISO 27001:2013 Information Security Management System. July 20, 2019. - Available at: https://isoconsultantkuwait.com/2019/07/20/2392 (датаобращения: 19.05.2021).

4. ProzorovA. ISMS Documented Information List, v.4.0. - Available at: https://vk.com/isms8020. (датаобращения: 19.05.2021).

5. ISMS Implementation Guideline/ A practical approach. - Available at: file:///C:/Users/1D1D~1/AppData/Local/Temp/1170.pdf (датаобращения: 19.05.2021).

6. ISO 27001: 2013 ISMS Documentation toolkit contents and ISO 27001: 2013 Requirement mapping //Document Control. – 2016. - No. 1. - pp.1-7.

7. COBIT 19 - URL: https://www.isaca.org/resources/cobit(дата обращения: 17.05.2021).

8. Rostami E., Karlsson F., Gao S. Requirements for computerized tools to design information security policies //Computers & Security. – 2020. - Vol. 99. - 102063.

9. Rose A., Okfalisac A. A. Information Security Policy Compliance: Systematic Literature Review // Procedia Computer Science. - 2019. - Vol. 161. - pp. 1216-1224.

10. Flowerday S. V., Tuyikeze T. Information security policy development and implementation: The what, how and who // Computers & Security. – 2016. - Vol. 61. - pp. 169-183.

11. Coertze J., von Solms R. A software gateway to affordable and effective Information Security Governance in SMMEs //Information Security for South Africa. - 2013. - pp. 1-8.

12. Rostami E., Karlsson F., Kolkowska E. The hunt for computerized support in information security policy management. Aliteraturereview //Information&ComputerSecurity. - 2020. - Vol. 28, No. 2. - pp. 215-259.

13. Суровцева Н. Г. Роботизированная документация: проблемы управления // Управление документами в цифровой экономике: Материалы научно-практич. конф. 5 декабря 2018 г. - М, 2019. - С. 23-30.

14. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management. – Available at: https://www.iso.org/standard/54533.html (датаобращения: 15.05.2021).

15. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance. – Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en. (датаобращения: 15.05.2021).

16. Information Security Awareness in Financial Organisations ENISA. – Available at: https://webcache.googleusercontent.com/search?q=cache:0Us-oaHURyQJ:https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport+&cd=1&hl=ru&ct=clnk&gl=ru(датаобращения: 15.05.2021).

17. Spitzner L. Defining the Security Awareness Maturity Model. – Available at: https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (датаобращения: 19.05.2021).

18. ENISA. Cyber Security Culture in organizations. 2017. - Available at: https://doi.org/10.2824/10543 (датаобращения: 19.05.2021).

19. Karlsson F., Åström J., Karlsson M. Information security culture–state-of-the-art review between 2000 and 2013 //Information & Computer Security. - 2015. - No. 23(3). - pp.246-285.

20. Mahfuth A., Yussof S., Baker A.A., Ali N. A systematic literature review: Information security culture // 2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS). DOI:10.1109/ICRIIS.2017.8002442 - Available at: https://www.researchgate.net/publication/319054554_A_systematic_literature_review_Information_security_culture (датаобращения: 19.05.2021).

21. Nasir A., Arshah R.A., Ab Hamid M. R., Fahmy S. An analysis on the dimensions of information security culture concept: A review //Journal of Information Security and Applications. – 2019. - No.44. - pp.12-22.

22. SANS Security Awareness Report. Building Successful Security Awareness Programs. 2018. - Available at: https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf(датаобращения: 18.05.2021).

23. ISO/IEC TS 33052:2016 Information technology. Process reference model (PRM) for information security management". - Available at: https://www.iso.org/standard/55142.html (датаобращения: 19.05.2021).

24. Sysoeva L.A. Using a reference model of processes in describing information security management processes in an organization. Information security: yesterday, today, tomorrow // Collection of articles based on the materials of the International Scientific and Practical Conference. –M., 2019. - pp. 59-65.

25. ISO / IEC TR 27008: 2011 "Information technology (IT). Methods and means of ensuring security. Recommendations for auditors regarding measures and means of control and management of information security." - URL: https://www.iso.org/ru/standard/45244.html(датаобращения: 19.05.2021).

References

1. InfoWatch. Restricted Information Leaks: 9 Months 2020 Report. - Available at: https://www.infowatch.ru/analytics/reports/30708 (accessed 31.03.2021).

2. ISO / IEC 27001-2013 Information technology - Security techniques - Information security management systems - Requirements. - Available at: https://www.iso.org/standard/54534.html (date accessed: 19.05.2021).

3. Biswas P. ISO 27001: 2013 Information Security Management System. July 20, 2019. - Available at: https://isoconsultantkuwait.com/2019/07/20/2392 (date accessed: 19.05.2021).

4. Prozorov A. ISMS Documented Information List, v.4.0. - Available at: https://vk.com/isms8020. (date of access: 19.05.2021).

5. ISMS Implementation Guideline / A practical approach. - Available at: file: /// C: /Users/1D1D~1/AppData/Local/Temp/1170.pdf (date accessed: 19.05.2021).

6. ISO 27001: 2013 ISMS Documentation toolkit contents and ISO 27001: 2013 Requirement mapping // Document Control. - 2016. - No. 1. - pp. 1-7.

7. COBIT 19 - URL: https://www.isaca.org/resources/cobit (date accessed: 17.05.2021).

8. Rostami E., Karlsson F., Gao S. Requirements for computerized tools to design information security policies // Computers & Security. - 2020. - Vol. 99. - 102063.

9. Rose A., Okfalisac A. A. Information Security Policy Compliance: Systematic Literature Review // Procedia Computer Science. - 2019. - Vol. 161. - pp. 1216-1224.

10. Flowerday S. V., Tuyikeze T. Information security policy development and implementation: The what, how and who // Computers & Security. - 2016. - Vol. 61. - pp. 169-183.

11. Coertze J., von Solms R. A software gateway to affordable and effective Information Security Governance in SMMEs // Information Security for South Africa. - 2013. - pp. 1-8.

12. Rostami E., Karlsson F., Kolkowska E. The hunt for computerized support in information security policy management. A literature review // Information & Computer Security. - 2020. - Vol. 28, No. 2. - pp. 215-259.

13. Surovtseva N. G. Robotic documentation: management problems // Document management in the digital economy: Materials of scientific and practical research. conf. December 5, 2018. - M, 2019.- pp. 23-30.

14. ISO / IEC 27002: 2013 Information technology - Security techniques - Code of practice for information security management. - Available at: https://www.iso.org/standard/54533.html (date accessed: 15.05.2021).

15. ISO / IEC 27003: 2017 Information technology - Security techniques - Information security management systems - Guidance. - Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en. (date of access: 15.05.2021).

16. Information Security Awareness in Financial Organizations ENISA. - Available at: https://webcache.googleusercontent.com/search?q=cache://Us-oaHURyQJ:https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/ fullReport + & cd = 1 & hl = ru&ct = clnk&gl = ru (date accessed: 15.05.2021).

17. Spitzner L. Defining the Security Awareness Maturity Model. - Available at: https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (date accessed: 19.05.2021).

18. ENISA. Cyber Security Culture in organizations. 2017. - Available at: https://doi.org/10.2824/10543 (date accessed: 19.05.2021).

19. Karlsson F., Åström J., Karlsson M. Information security culture – state-of-the-art review between 2000 and 2013 // Information & Computer Security. - 2015. - No. 23 (3). - pp. 246-285.

20. Mahfuth A., Yussof S., Baker A.A., Ali N. A systematic literature review: Information security culture // 2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS). DOI: 10.1109 / ICRIIS.2017.8002442 - Available at: https://www.researchgate.net/publication/319054554_A_systematic_literature_review_Information_security_culture (date accessed: 19.05.2021).

21. Nasir A., Arshah R. A., Ab Hamid M. R., Fahmy S. An analysis on the dimensions of information security culture concept: A review // Journal of Information Security and Applications. - 2019. - No.44. - pp.12-22.

22. SANS Security Awareness Report. Building Successful Security Awareness Programs. 2018. - Available at: https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf (date accessed: 18.05.2021).

23. ISO / IEC TS 33052: 2016 Information technology. Process reference model (PRM) for information security management."- Available at: https://www.iso.org/standard/55142.html (date accessed: 19.05.2021).

24. Sysoeva L.A. Using a reference model of processes in describing information security management processes in an organization. Information security: yesterday, today, tomorrow // Collection of articles based on the materials of the International Scientific and Practical Conference. - M., 2019. - pp. 59-65.

25. ISO / IEC TR 27008: 2011 "Information technology (IT). Methods and means of ensuring security. Recommendations for auditors regarding measures and means of control and management of information security." - URL: https://www.iso.org/ru/standard/45244.html (date of access: 19.05.2021).

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: astakhovalv@susu.ru

КИРЯЕВ Андрей Игорьевич, студент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: andkir0408@gmail.com

ASTAKHOVA Liudmila Victorovna, Doctor of Pedagogy, Professor, Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: astakhovalv@susu.ru

KIRYAEV Andrey Igorievich, student of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: andkir0408@gmail.com