УДК 33 **DOI: 10.34670/AR.2022.76.11.015**

Анализ рисков информационной безопасности в информационной системе текстильной промышленности Эритреи

Асфха Амануал Эстифанос

Аспирант,
Национальный исследовательский университет ИТМО,
197101, Российская Федерация, Санкт-Петербург,
Кронверкский пр., 49;
e-mail: pressa@itmo.ru

Аннотация

До настоящего времени предпринимались многочисленные попытки классифицировать угрозы информационной безопасности, особенно в промышленной сфере. Однако до сих пор существует множество неизвестных рисков, которые могут угрожать безопасности текстильной индустрии и ее ресурсов. Цель настоящего исследования заключалась в оценке рисков, угрожающих информационной безопасности в текстильной промышленности, расположенной в одном из центральных городов Эритреи. Это исследование было завершено в 2021 году. Его участниками были IT-менеджеры и эксперты по управлению рисками, работавшие в текстильной промышленности (n = 15). Идентификации рисков были собраны с помощью анкетирования и интервью, состоящего из ряда вопросов с использованием методов качественного и количественного анализа рисков. Анализ рисков является одним из ключевых этапов процесса управления рисками: выявление рисков, определение и оценка всех возможных рисков. Результаты показали, что среди рисков информационной безопасности физическое оборудование: A2 находятся в состоянии Угрозы с перебоями питания, что является фактором риска с высокой вероятностью; Управление человеческими ресурсами: A5 (Персонал), находящиеся в состоянии болезни, является фактором риска низкого воздействия с низкой вероятностью. Элементы риска высокой вероятности требуют немедленных корректирующих действий. В результате, прежде чем испытывать негативные последствия, следует признать и контролировать основные источники таких опасностей. Стоит также отметить, что информационная безопасность в текстильных промышленных системах должна рассматриваться в рамках первичных интересов и политики на глобальном уровне.

Для цитирования в научных исследованиях

Асфха А.Э. Анализ рисков информационной безопасности в информационной системе текстильной промышленности Эритреи // Экономика: вчера, сегодня, завтра. 2022. Том 12. № 2А. С. 126-134. DOI: 10.34670/AR.2022.76.11.015

Ключевые слова

Текстильная информационная система, информационная безопасность, риски, анализ и оценка рисков, информационная система.

Введение

Подавляющее большинство фирм в настоящее время уязвимы перед рядом внутренних и внешних угроз безопасности, таких как подделка и кража данных. Другие угрозы безопасности могут включать стихийные бедствия и непреднамеренные ошибки пользователей компьютеров, которые могут иметь катастрофические последствия [ISO/IEC 27000, 2018].

Проблемы информационной безопасности касаются как текстильного сектора, так и других предприятий. В тоже самое время им предлагается использовать информацию об электронном секторе и обмениваться ею. Из-за высокой ценности отраслевых данных они особенно уязвимы к нарушениям данных. В результате, защита отраслевой информации в организациях текстильной промышленности представляется более сложной задачей, чем раньше.

В связи с быстрыми технологическими разработками в вычислительных устройствах все системы промышленной обработки, заводы, машины, испытательные установки, (помещения, аппаратура, программное обеспечение, принадлежности, документация, данные и т.д.) сместились или превратились из механизации в автоматизацию.

Возможность управления рисками сегодня является центральной проблемой в любой бизнес-сфере или отрасли. Это ведет нас к управлению безопасностью, и тому, почему промышленные организации должны обеспечивать наличие систем управления информационной безопасностью. Системы управления информационной безопасностью (СУИБ) сохраняют конфиденциальность, целостность и доступность информации [Модель управления рисками…, 2014] путем применения процесса управления рисками и обеспечивают гарантии заинтересованным сторонам, что риски в достаточной степени управляются.

В результате, цель управления рисками информационной безопасности заключается в обеспечении безопасности систем, которые хранят, обрабатывают или передают организационные данные [Ло, 2012]. Должен быть разработан план анализа серьезности угроз и определения потенциальных опасностей для управления рисками [Методологии информационной безопасности…, 2005]. Оценка рисков или анализ рисков фактически являются начальным этапом процесса управления рисками [Ло, 2012; Схема для сравнения…, 2005].

Выявление угроз и уязвимостей, анализ вероятности и воздействия, связанных с известными угрозами, и, наконец, определение приоритетности рисков для определения соответствующего уровня обучения и контроля, необходимых для эффективного смягчения – все это методы оценки рисков информационной безопасности [Шамала, 2013].

Целью этой работы является оценка уязвимостей информационной безопасности в текстильной промышленности с использованием стандарта ISO 27005. Результаты этого исследования могут быть использованы для повышения эффективности работы отдела информационных технологий и информационной безопасности текстильной промышленности.

После рассмотрения, обоснования и утверждения руководством завершенного проекта, мы суммируем пять наиболее ценных активов. Это Чистая информация в виде электронных данных: A1 (данные в состоянии покоя, данные в использовании и данные в движении), физическое оборудование: A2 (главным образом, серверы и электроника конечного пользователя, и оборудование, используемое в текстильной промышленности.... и т.д.), которые обеспечивают технические опорные платформы, вспомогательные платформы, на которых работает вся организация, система управления доходами от программного обеспечения: A3 (RMS) используется для обработки бизнес-информационных процессов и управления ими, текстильная

промышленность – Репутация: A4 (нематериальные активы) и Управление человеческими ресурсами: A5 (персонал или работодатели), которые являются основой для успешного функционирования текстильной промышленности и также являются самым слабым звеном в цепочке обеспечения безопасности.

Методы исследования

Это было исследование методов анализа рисков ISSRAM на основе ISO 27005, которое было завершено в 2021 году. Участниками стали менеджеры отделов информационных технологий текстиля, расположенных в одном из городов в центре Эритреи Асмэра (n = 15). Поэтому в этом небольшом исследовании приняли участие 15 IT-менеджеров и полевых экспертов. Пятнадцать (15) участников имели хорошие теоретические знания и отличные практические навыки в текстильной промышленности и управлении рисками. Эти участники имели промежуточное или выше техническое звание, имели степень бакалавра или выше и имели более чем 5-летний опыт работы в профессии. Каждому из участников было предложено определить вероятность и влияние возникновения угрозы или риска на пять баллов шкалы Лайкерта, таких как (очень низкий = 1, Низкий = 2, Средний = 3, Высокий = 4 и Очень высокий = 5). Содержание и первичную обоснованность анкеты подтвердили два эксперта в области управления текстильной информацией и электротехники.

Для анализа данных автором был использован подход ISSRM (метод управления рисками информационной безопасности). Он помогает определить, какие активы являются ценными и требуют защиты от конкретных опасностей. Кроме того, в нем предлагаются альтернативные меры по устранению рисков в форме контрмер по обеспечению безопасности. Он включает модель домена, ключевые показатели и процесс управления рисками.

Первая причина выбора метода управления рисками информационной безопасности заключалась в его качественном характере, который отличает его от других методов. Вторая причина заключается в том, что он напоминает методологию оценки информационных рисков 2 (IRAM2).

Анкета и интервью состояли из трех разделов: персональная информация, характеристики систем и статус информационной безопасности в текстильной промышленности (контекст) и выявление рисков (этот раздел включал стихийные бедствия, угрозы для человека и физические/экологические угрозы).

Метрики

Методика метода управления рисками информационной безопасности [Дюбуа, 2010] обеспечивает ряд метрик.

Во-первых, показатель стоимости описывает стоимость промышленного актива с точки зрения потенциального воздействия, если он выявлен, изменен или нарушен.

Во-вторых, показатель потребности в обеспечении указывает, насколько важен критерий обеспечения с точки зрения промышленного актива. Эти два показателя используются для характеристики понятий активов.

В завершении, метрика правдоподобия учитывает цель противника и сложность метода атаки для определения возможности нападения. Статистика уровня уязвимости отражает, насколько широко распространена уязвимость и насколько вероятно ее использование.

Основная часть

Уравнение 1 представляет метрики вероятности и уровня уязвимости, которые используются для оценки потенциала. Максимальное значение, введенное в меру необходимости безопасности, является метрикой уровня воздействия.

Потенциал = Вероятность + Уязвимость - 1 …… (1)

Продукт потенциала и уровня воздействия используется для создания показателя уровня риска.

Уровень риска = Потенциал × Воздействие……. (2)

Процесс метода управления рисками информационной безопасности

В настоящем документе предлагаются данные для проведения анализа рисков для текстильной информационной системы на предприятиях путем принятия методологии методом управления рисками информационной безопасности. Исходя из этого, в эритрейской текстильной промышленности были проведены тематические исследования с целью выявления возможных рисков для информационной безопасности, и с использованием рекомендованного подхода к анализу рисков эти риски были снижены до приемлемого уровня. Проведение оценки рисков включает количественную оценку всех элементов процесса, включая определение активов и их стоимости, воздействия, частоты угроз, эффективности и стоимости защиты, неопределенности и вероятности. Это включает в себя семь основных шагов, но в этом исследовании автор дошел только до шестого шага из-за ограниченного объема исследовательской работы.

Шаг 1: Определение актива и его стоимости для каждого информационного актива.

Шаг 2: Выявление угроз для актива и оценка вероятности угроз.

Шаг 3: Определение уязвимости по отношению к активу и оценка уровня уязвимости.

Шаг 4: Оценка потенциала.

Шаг 5: Оценка уровня воздействия.

Шаг 6: Оценка уровня риска.

Шаг 7: Предполагаемое решение.

Определение активов и их стоимости

Мы рассматриваем стоимость активов (включая информацию), объем работ по их разработке, затраты на их содержание, ущерб, причиненный в случае их утраты или уничтожения, и выгоды, которые получит другая сторона, если получит их в процессе идентификации активов и их стоимости. Выявление промышленного актива и оценка его стоимости являются важным шагом в определении надлежащего уровня защиты.

Стоимость актива для любого отраслевого сектора может быть как количественной (связанной с его стоимостью), так и качественной (связанной с его производительностью).

Идентификация и анализ угроз:

Угроза – это кто-то, что-то, событие или идея, которая создает или представляет риск для актива.

Угрозы могут раскрыть конфиденциальность, целостность и доступность активов, используя уязвимости или состояние слабости.

После выявления активов, которые необходимо защитить или обеспечить, необходимо признать или выявить опасность для этих активов, а также оценить риск убытков.

Анализ угроз – это процесс изучения источников киберугроз и оценки их уязвимости информационной системы. Цель исследования – выявить угрозы, которые ставят под угрозу

конкретную информационную систему в данной среде.

Он состоит из четырех этапов, которые включают в себя:

– Определить фактическую угрозу.

– Определить возможные последствия для организации в случае возникновения угрозы.

– Определить вероятную частоту угрозы.

– Оценить вероятность того, что угроза осуществится.

Выявление уязвимости по отношению к активу

Уязвимость описывается как недостаток или отсутствие безопасности в системе безопасности. Угрозы могут использовать ситуацию уязвимости, потому что она предоставляет или создает возможность для них. Для определения четкого уровня риска изучаются взаимосвязи между угрозами и уязвимостями. Уязвимости – это характеристики определенных активов информационной системы, которые может использовать угроза.

Результаты исследования

Как указывалось ранее, в этом опросе приняли участие IT-менеджеры и специалисты по управлению рисками из текстильного сектора (n = 15). Участниками были люди (34,33 ± 6,79) лет в среднем, причем большинство из них были мужчины (73,33%, n = 11). Более половины участников (80%, n = 12) имели отношение к компьютерным наукам и электротехники. С точки зрения опыта работы, большинство участников (60%, n = 9) имели менее десяти лет опыта.

Идентификация активов, угроз и уязвимостей:

Таблица 1 - Взаимосвязь между активами, угрозами и уязвимостями для таблицы анализа метода управления рисками информационной безопасности

Актив	Код угрозы	Угроза	Уязвимость	Код уязвимости
A1	T1	Внедрение SQL-кода	Устаревшая СУБД	У1
	T2	Ошибка пользователя	Халатность	У2
A2	T3	Прерывание питания	Невозможность работы без источника питания	У3
	T4	Пожар	Уязвимая физическая проблема/повреждение	У4
A3	T5	Межсайтовые сценарии	Восприимчивость к вредоносному коду	У5
	T6	Отказ в обслуживании	Недостаточный объем памяти	У6
A4	T7	Мошенничество	Нечестность персонала	У7
	T8	Нецелевое использование ресурсов	Просчеты в управлении ресурсами	У8
A5	T9	Несчастные случаи	Несоблюдение мер безопасности	У9
	T10	Болезнь	Болезнь из-за смены погоды	У10

Таблица 2 - Таблица оценки рисков

Актив	Значение актива	Угроза	Вероятность угрозы	Уровень уязвимости	Потенциал	Воздействие	Уровень риска
A1	4.2	T1	3.4	4.2	6.6	3.9	25.74
		T2	4.2	3	6.2	3.2	19.84

Актив	Значение актива	Угроза	Вероятность угрозы	Уровень уязвимости	Потенциал	Воздействие	Уровень риска
A2	4.8	T3	3.9	4.7	7.6	4.3	32.68
		T4	4.1	4.3	7.4	3.8	28.12
A3	2.2	T5	2.9	2.2	4.1	3.3	13.53
		T6	2.6	2.7	4.3	4.1	17.63
A4	3.3	T7	3.7	3.3	6	2.9	17.40
		T8	1.9	3.2	4.1	3.2	13.12
A5	1.5	T9	2	1.8	2.8	3.7	10.36
		T10	1.2	2	2.2	2	4.40

Значения активов, вероятности угроз и уровня уязвимости были получены посредством оценок экспертных заключений, которые приведены в таблице 2.

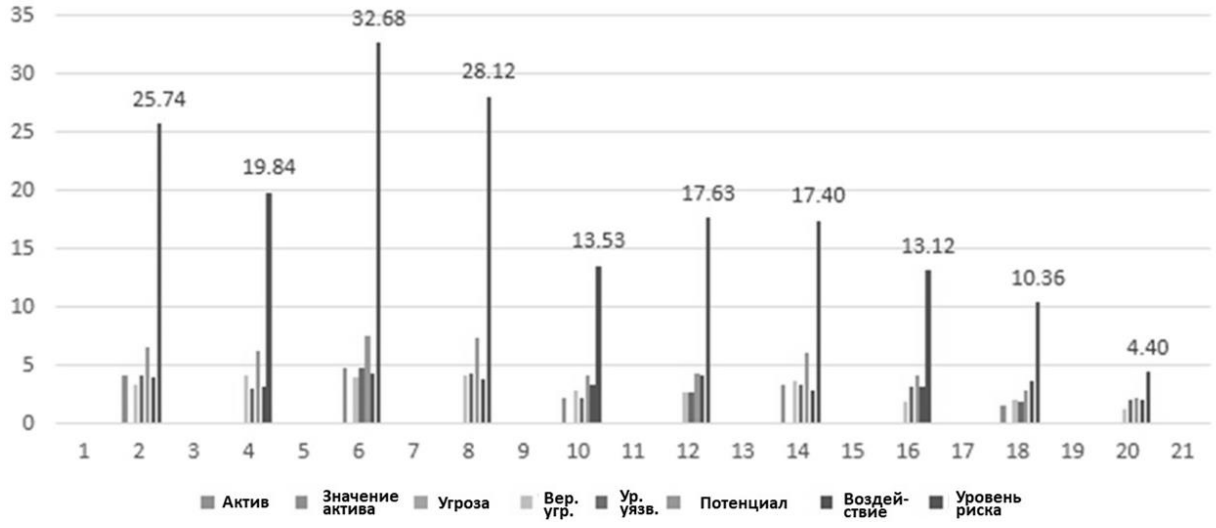

Рисунок 1 - Уровень риска

Анализ рисков является одним из ключевых этапов процесса управления рисками: выявление рисков, оценка всех возможных рисков. Результаты показали, что среди рисков информационной безопасности физическое оборудование: A2 находятся в состоянии Угрозы с перебоями питания (T3), что является фактором риска с высокой вероятностью (32.68); Управление человеческими ресурсами: A5 (Персонал), находящиеся в состоянии болезни (T10), является фактором риска низкого воздействия с низкой вероятностью (4.4). Поэтому, согласно этой оценке риска, элементы риска высокой вероятности требуют немедленных корректирующих действий для снижения риска в текстильной промышленности.

Ограничение: в данной работе был выявлен некоторый недостаток. Прежде всего, данные для этого исследования были собраны из текстильной промышленности Эритреи, которая расположена в одном из городов Эритреи (Асмара). Хотя результаты этого исследования могут быть применимы только к условиям исследования, доступность метода исследования может помочь другим исследователям в изучении проблем информационной безопасности в других контекстах.

Некоторым другим недостатком может быть небольшое число людей, принявших участие в исследовании. Исследование, действительно, было сделано в одном из городов Эритреи из-за ограничений по времени и затратам. Дальнейшие исследования с большим размером выборки и

в различных ситуациях рекомендуются для проверки пригодности анкеты и оценки вероятности и воздействия угроз.

Заключение

Таким образом, мы определили пять ключевых активов организации, таких как электронные данные, оборудование, репутация организации, программное обеспечение Сервиса подбора персонала и Управления человеческими ресурсами. Основными угрозами, с которыми сталкиваются эти активы, являются внедрение SQL-кода, межсайтовые сценарии, мошенничество, аварии и перебои с питанием, которые являются причиной наиболее серьезных угроз информационной безопасности в организации. Для предотвращения, обнаружения, смягчения и уменьшения использования уязвимостей, обнаруженных с помощью активов, применяются соответствующие отраслевые стандарты административного, технического и физического контроля.

Элементы с высокой вероятностью опасности требуют немедленных корректирующих действий. В результате, прежде чем испытывать негативные последствия, следует признать и контролировать основные источники таких опасностей. Стоит также отметить, что информационная безопасность в текстильных промышленных системах должна рассматриваться в рамках первичных интересов и политики на глобальном уровне.

Библиография

1. Бодин Л.Д. Оценка инвестиций в информационную безопасность с использованием метода аналитической иерархии. 2005.
2. Гоэль С., Чен В. Матричные методологии анализа рисков информационной безопасности. Нью-Йорк, 2005.
3. Джейсон М. Инструментарий оценки рисков информационной безопасности. Сингресс, 2013.
4. Дюбуа Э. и др. Системный подход к определению предметной области управления рисками безопасности информационных систем // Преднамеренные взгляды на разработку информационных систем. Берлин, 2010. С. 289-306.
5. Кузьминых Е. Оценка рисков информационной безопасности. 2021.
6. Ло С. Гибридная система оценки рисков информационной безопасности (HISRAS) с учетом взаимозависимостей между элементами управления. 2012.
7. Методологии информационной безопасности, а также системы и требования по управлению информационной безопасностью согласно ISO 27001:2005. 2005
8. Модель управления рисками: количественные и качественные аспекты. Решения для управления. 2014.
9. Шамала П. Теоретическая основа информационной структуры для оценки рисков информационной безопасности. 2013.
10. ISO/IEC 27000: Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности – ISO/IEC 27005:2018 и стандарт ISO. Женева, 2018.

Analysis of information security risks in the information system of the textile industry of Eritrea

Asfha Amanual Estifanos

Postgraduate,
ITMO University,
197101, 49, Kronverkskii ave., St. Petersburg, Russian Federation;
e-mail: pressa@itmo.ru

Abstract

To date, numerous attempts have been made to classify threats to information security, especially in the industrial sphere. However, there are still many unknown risks that may threaten the safety of the textile industry and its resources. The purpose of this study was to assess the risks threatening information security in the textile industry located in one of the central cities of Eritrea. This study was completed in 2021. Its participants were IT managers and risk management experts working in the textile industry (n = 15). Risk identifications were collected through questionnaires and interviews consisting of a number of questions using methods of qualitative and quantitative risk analysis. Risk analysis is one of the key stages of the risk management process: identification of risks, identification and assessment of all possible risks. The results showed that among the risks of information security, physical equipment: A2 are in a state of Threat with power outages, which is a risk factor with a high probability; Human resource management: A5 (Personnel) who are in a state of illness is a risk factor of low impact with a low probability. Elements of high probability risk require immediate corrective actions. As a result, before experiencing negative consequences, the main sources of such dangers should be recognized and controlled. It is also worth noting that information security in textile industrial systems should be considered within the framework of primary interests and policies at the global level.

For citation

Asfkha A.E. (2022) Analiz riskov informatsionnoi bezopasnosti v informatsionnoi sisteme tekstil'noi promyshlennosti Eritrei [Analysis of information security risks in the information system of the textile industry of Eritrea]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 12 (2A), pp. 126-134. DOI: 10.34670/AR.2022.76.11.015

Keywords

Textile information system, information security, risks, risk analysis and assessment, information system.

References

1. Bodin L.D. (2005) *Otsenka investitsii v informatsionnuyu bezopasnost' s ispol'zovaniem metoda analiticheskoi ierarkhii* [Evaluation of investment in information security using the method of analytical hierarchy].
2. Dubois E. et al. (2010) Sistemnyi podkhod k opredeleniyu predmetnoi oblasti upravleniya riskami bezopasnosti informatsionnykh sistem [A systematic approach to defining the subject area of information systems security risk management]. In: Prednamerennye vzglyady na razrabotku informatsionnykh sistem [Intentional views on the development of information systems]. Berlin.
3. Goel S., Chen V. (2005) *Matrichnye metodologii analiza riskov informatsionnoi bezopasnosti* [Matrix Methodologies for Information Security Risk Analysis.]. New York.
4. Jason M. (2013) *Instrumentarii otsenki riskov informatsionnoi bezopasnosti* [Information Security Risk Assessment Toolkit]. Singress.
5. (2018) *ISO/IEC 27000: Informatsionnye tekhnologii – Metody obespecheniya bezopasnosti – Upravlenie riskami informatsionnoi bezopasnosti – ISO/IEC 27005:2018 i standart ISO* [ISO/IEC 27000: Information technology –Security practices – Information security risk management – ISO/IEC 27005:2018 and the ISO standard]. Geneva.
6. Kuz'minykh E. (2021) *Otsenka riskov informatsionnoi bezopasnosti* [Information security risk assessment].
7. Lo S. (2012) *Gibridnaya sistema otsenki riskov informatsionnoi bezopasnosti (HISRAS) s uchetom vzaimozavisimostei mezhdu elementami upravleniya* [Hybrid Information Security Risk Assessment System (HISRAS) considering interdependencies between controls. 2012. Information security methodologies, as well as information security management systems and requirements in accordance with ISO 27001:2005. 2005].
8. (2005) *Metodologii informatsionnoi bezopasnosti, a takzhe sistemy i trebovaniya po upravleniyu informatsionnoi bezopasnost'yu soglasno ISO 27001:2005* [Information security methodologies, as well as information security management systems and requirements in accordance with ISO 27001:2005].

9. (2014) *Model' upravleniya riskami: kolichestvennye i kachestvennye aspekty. Resheniya dlya upravleniya* [Risk management model: quantitative and qualitative aspects. Management solutions].
10. Shamala P. (2013) Teoreticheskaya osnova informatsionnoi struktury dlya otsenki riskov informatsionnoi bezopasnosti [An Information Framework Theoretical Framework for Information Security Risk Assessment].