ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.53

DOI: 10.21822/2073-6185-2025-52-2-122-129 Оригинальная статья / Original article

Защита информационных потоков коммерческого назначения на промышленном предприятии

И.А. Лоскутов, С.Е. Акатов

[1]Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы имени А.Г. Иосифьяна» (АО Корпорация «ВНИИЭМ»),
[1]107078, г. Москва, ул. Вольная, 30, стр. 10, Россия,
[1]Колледж экономики, права и информационных технологий,
[1]109029, г. Москва, ул. Нижегородская, 32, стр.16, Россия,
[1]МИРЭА - Российский технологический университет,
[1]119454, г. Москва, проспект Вернадского, 78, стр.4, Россия,
[2]ПАО «МАК» «Вымпел»,
[2]125167, г. Москва, ул. 4 –я Восьмого марта, 3, Россия

Резюме. Цель. Целью исследования является обобщение имеющихся сведений по проблеме обеспечения защиты информации на промышленным предприятиях, работающих исключительно с коммерческой тайной. **Метод**. Методы научного познания, использованные при написании работы: систематизация, анализ, описание, прогноз. **Результат.** Из открытых источников проведен анализ потребности в формировании модели защиты; дан прогноз потенциального ущерба. Сформирована концептуальная модель объекта защиты; сгруппированы входящие подразделения промышленного предприятия по признаку вероятности возникновения компьютерной атаки. Доказана значимость формирования модели защиты, описан процесс формирования организационной структуры промышленного предприятия. **Вывод**. Полученные в работе выкладки позволяют оценить динамику роста ущерба от компьютерной атаки, тем самым доказывая важность подобных исследований. Результаты исследования дают обоснование неоправданности применения некоторых мер с точки зрения защиты информации коммерческого назначения.

Ключевые слова: защита информации, предприятие, коммерческая тайна, промышленность, информационная безопасность, модель защиты информации

Для цитирования: И.А. Лоскутов, С.Е. Акатов. Защита информационных потоков коммерческого назначения на промышленном предприятии. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(2):122-129. DOI:10.21822/2073-6185-2025-52-2-122-129

Protection of commercial information flows in an industrial enterprise

I.A. Loskutov, S.E. Akatov

[1]A.G. Iosifian' Joint Company 'Research and Production Corporation "Space Monitoring Systems, information management and electromechanical complexes",
[1]30 Volnaya St., p. 10, Moscow 107078, Russia,
[1]College of Economics, Law and Information Technology,
[1]32 Nizhegorodskaya St., build.16, Moscow 109029, Russia,
[1]MIREA - Russian Technological University,
[1]78, Vernadsky Ave., build.4, Moscow 119454, Russia,
[2]PAO "MAK" "Vympel",
[2]3, 4th Vosmogo Marta St., Moscow 125167, Russia

Abstract. Objective. The aim of the study is to summarize the available information on the problem of ensuring information security at industrial enterprises working exclusively with commercial secrets. **Method.** The methods of scientific knowledge used in writing the work: systematization, analysis, description, forecast. **Result.** The analysis of the need for forming a protection model was conducted from open sources; a forecast of potential damage was given. A conceptual model of the protected object was formed; the incoming divisions of the industrial enterprise were grouped according to the probability of a computer attack. The importance of forming a protection model was proven, the process of forming the organizational structure of an industrial enterprise and a protection model was described. **Conclusions.** The calculations obtained in the work allow us to estimate the dynamics of damage growth from a computer attack, thereby proving the importance of such studies. The results of the study provide a rationale for the unjustified use of certain measures when considering production from the point of view of protecting commercial information.

Keywords: information protection, enterprise, trade secret, industry, information security, information protection model

For citation: I.A. Loskutov, S.E. Akatov. Protection of commercial information flows in an industrial enterprise. Herald of Daghestan State Technical University. Technical Sciences.2025;52(2):122-129. (In Russ) DOI:10.21822/2073-6185-2025-52-2-122-129

Введение. Большинство сведений, хранимых, обрабатываемых и исполняемых на всевозможных АРМах, серверах, оборудовании и других технических устройствах современного промышленного предприятия зачастую носят коммерческий характер, за исключением случаев, где превалирует гостайна. Принципы процессного распределения в них аналогичны[1]. В последние десятилетия наблюдается рост компьютерных атак [2]. Промышленные предприятия также подпадают под них, что вынуждает правообладателей информации искать способы противодействия, искать пути поведенческого моделирования, как, например, указано в [3]. Безусловно, в Российской Федерации имеет место наличие большого количества нормативно-правовых актов по направлению [4], однако законодательная база не может явно обеспечить сохранность информации. Преступник, в лучшем случае, понесет заслуженное наказание, но прибыль, авторитет предприятия могут быть частично, а в худшем случае безвозвратно потеряны [5]. От того вопросы защиты информации (ЗИ) ложатся на плечи собственников информации, государство же пытается максимально предоставить сведения, необходимые для обеспечения ее сохранности, формируя портальные сведения – банк угроз [6] и т.п.

Постановка задачи. Для комплексного обеспечения защиты информации, необходимо не только структурировать разрозненные материалы относительно злоумышленников и их возможностей, но и также понимать, в каком направлении с большей или меньшей вероятностью будет проходить КА, в каких подразделениях АРМы, технические средства будут наиболее подвержены угрозам. Таким образом начинает формироваться потребность в разработке модели защиты промышленного предприятия; требуется рассмотреть комплексно как внутренние процессы, так и интерес со стороны к ним, обозначить важность разрабатываемой модели. Решение отмеченных задач крайне актуально на данный момент, т.к. нет единого подхода.

Методы исследования. Доказательство значимости формирования модели защиты. На промышленном предприятии, как уже было отмечено, находится много всевозможных контуров, обеспечивающих должный уровень функционирования внутренних процессов производства, потому и обеспечение ЗИ, курсирующей в них становится все более актуальной задачей с учетом возрастающих киберугроз. Однако, не стоит думать, что данный процесс тривиален, именно комплекс мер по максимизации недопущения киберинцендентов и формирует ЗИ [7]. Для создания должной модели защиты необходимо проверить гипотезу о важности данных деяний. В данном случае был проведен статистический

анализ кибернападений, показанный в [8]. Количество атак неизменно растет, однако рационально также определить процентное соотношение. На конец 2022 года в Российской Федерации было зарегистрировано порядка 2,4 млн. компаний [9], из которых на промышленное производство приходилось 238,77 тыс. (10,01% из общего числа).

Оценим вероятность возникновения киберугрозы. Для этого возьмем данные по IV кварталу 2022 года, т.к. они наиболее верно соотносятся со сведениями о количестве фирм на отечественном рынке. Уравнение примет вид:

$$P_{\text{КА}} = \frac{281000}{2382660} * 0{,}1001 \approx 0{,}0118 \Rightarrow 1{,}18\% \quad (1)$$

где: $P_{\text{КА}}$ – вероятность возникновения кибератаки на предприятии; 281000 – количество КА в IV квартале 2022 года; 2383660 – общее количество компаний на конец 2022 года; 0,1001 – процент промышленных предприятий (10,01%).

Однако, безусловно, расчет достаточно грубый, не исключено проведение нескольких КА на одно производство, кроме того, не стоит обходить вниманием тот факт, что полученное значение показывает только вероятность проведения атаки, а не ее успешное завершение. Отметим, что чистых цифр по количеству успешных КА в интернет пространстве мало. Наиболее подробная, на наш взгляд, информация была показана на графике в работе [10], однако ее значения разнятся с некоторыми источниками, например, с [11]. Потому далее на базе косвенных данных проведем оценку увеличения успешных КА.

На основании сведений из [11], в 2022 году прошло увеличение «успешных» КА на 56%. В качестве упрощения, примем количество КА на конец 2021 года равным значению I квартала 2022 года. Т.о., соотношение будет следующим:

$$\begin{cases} Perc_{\text{КА}_{2021}} = \frac{N_{\text{КА}_{2021}}}{180000} \\ Perc_{\text{КА}_{2022}} = \frac{N_{\text{КА}_{2022}}}{281000} \\ Perc_{\text{КА}_{2021}} * 1.56 = Perc_{\text{КА}_{2022}} \end{cases} \quad (2)$$

где: $Perc_{\text{КА}_{2021}}$, $Perc_{\text{КА}_{2022}}$ – процент КА в 2021 и 2022 году; $N_{\text{КА}_{2021}}, N_{\text{КА}_{2022}}$ – количество успешных КА в 2021 и 2022; 1,56 – учет увеличения на 56 % количества успешных КА. В результате, $N_{\text{КА}_{2022}}$ стал в ≈ 2,44 раза больше, чем $N_{\text{КА}_{2021}}$.

При условии допущения, что всего лишь 1/1000 из КА достигала цели в 2022 году, ее вероятность будет: $P_{\text{УспКА}} = 1{,}18\% * 0{,}001 \approx 0{,}002\%$ (3)

где: $P_{\text{УспКА}}$ – вероятность успешности КА на промышленном предприятии; 0,001 – приблизительное соотношение успешности КА в 2022 года относительно промышленных предприятий.

Однако, при сохранении динамики, данный параметр будет меняться по логике рис. 1.

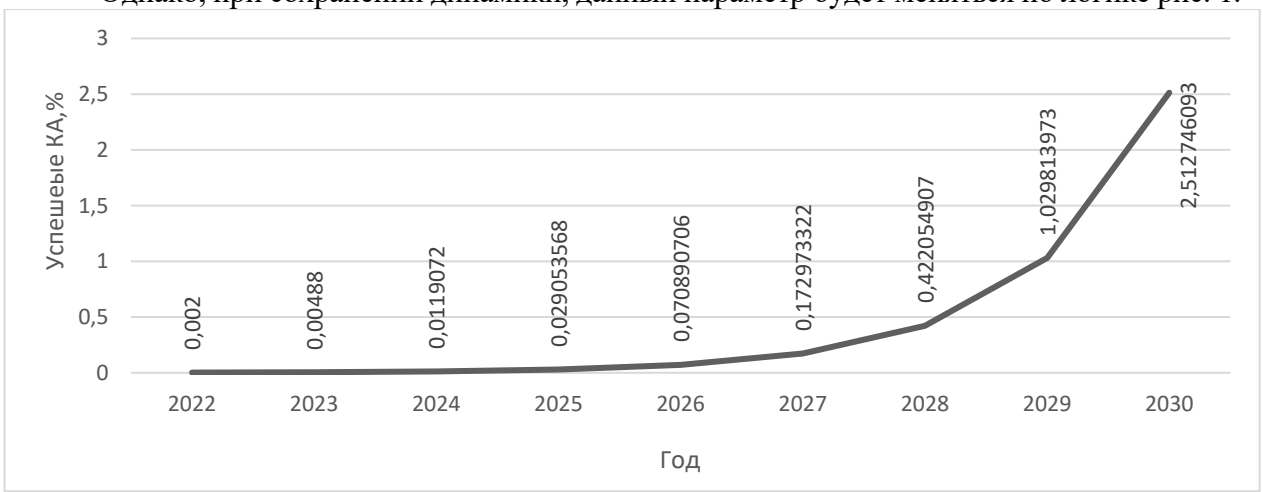

Рис. 1 – Прогнозируемое количество успешных КА
Fig. 1 - Predicted number of successful CA

С учетом, что на 2022 год потери по [12] у компаний составили 20 млн. руб., при условии стабильности на одну успешную КА, график средних потерь при совмещении с рис. 1 будет таким (рис. 2).

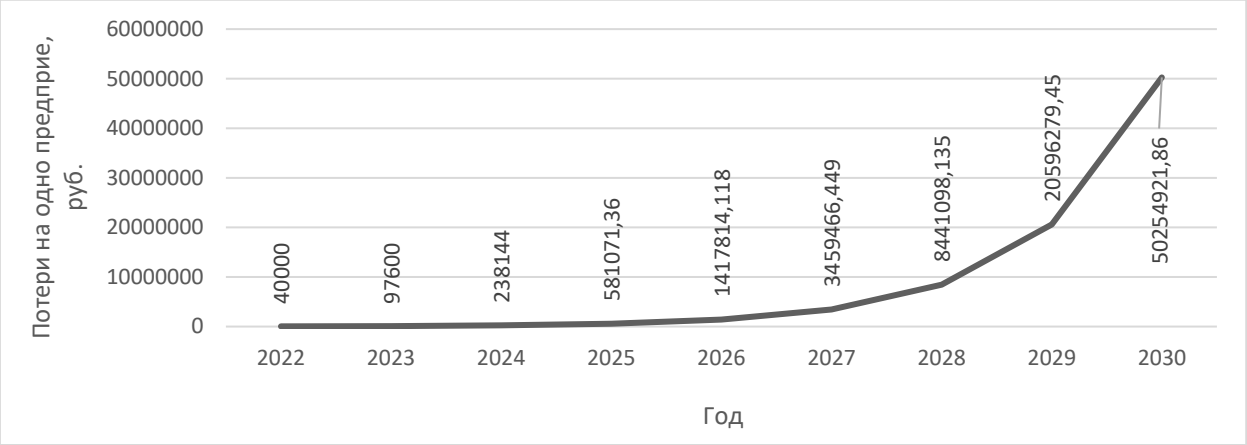

Рис. 2 – График средних потерь на одну компанию от КА
Fig. 2 - Schedule of medium losses per company from CA

На графике видно, что потери стабильны и равны известным ранее 20 млн руб., однако в реальности цифры будут много больше по понятным причинам.

Важно отметить, что несмотря на малое значение, приходящееся в целом на единичное предприятие, оно достаточно сильно влияет на ее экономику, т.к. ущерб не усреднен. Кроме того, как можно заметить, в потенциале суммы очень значительно вырастут.

Отмеченные выкладки полностью доказывают важность борьбы с киберпреступниками. Для обеспечения должного уровня ИБ необходимо понимать, что обязательно должно быть сделано на промышленном предприятии, чтобы свести вероятность возникновения киберугрозы к минимуму.

Поэтому, далее можно непосредственно перейти к формированию модели защиты.

Формирование типовой организационной структуры промышленного предприятия. Как известно, промышленное предприятие состоит из достаточно большого количества различных организационных единиц. В следствие постоянного роста киберпреступлений [13], значимая доля которых приходится на рассматриваемые организационные единицы [14], важно определить их базис-состав.

Безусловно, на данный момент времени накопилось достаточное количество информации относительно функционирования входящих в него структурных компонентов. Наиболее удобным для рассмотрения следует считать наработки, показанные в работе [15]. Причиной выбора является оптимальное углубление и дробление организационной структуры.

Так, на основании отмеченных материалов, модель типового предприятия будет из себя представлять порядка 18 базис-частей. Отдельно отметим, что в случае дивизионального характера организационной структуры, свойственной корпорациям и иным конгломератным объединениям, возможна надстройка, однако она будет или дублирующей, или же расширенной в виде генерального директора дивизиона и т.п., по аналогичной логике.

Исследование проводилось с точки зрения обеспечения ЗИ из работы [15] с присуждением трех уровневой категории значимости обеспечения ИБ. Результат сведен в табл. 1. Таким образом, была создана уровневая градация подразделения, необходимая для последующего распределения сил службы ИБ в КИИ.

Обсуждение результатов. Формирование модели защиты. Для обеспечения должного уровня ЗИ были определены минимальные требования к ИБ на промышленном предприятии. В данном случае это: ИАФ: 1, 3, 4, 5, 6. Опишем причины отсутствия 2 и 7 позиций.

Таблица 1 – Вероятность кибератаки на подразделение
Table 1 – The probability of cyber attack on the unit

Подразделение Division	Уровень Level			Подразделение Division	Уровень Level		
	Низкий Low	Средний Medium	Высокий High		Низкий Low	Средний Medium	Высокий High
Экспериментальный цех Experimental shop			+	Инструментальный цех Tool shop	+		
Ремонтномеханический цех Repair and mechanical shop	+			Электромеханический цех Electromechanical shop		+	
Основные производственные цехи Main production shops			+	Планово-диспетчерский отдел Scheduling and dispatching department			+
Отдел главного технолога Chief technologist departments			+	Отделы главного механика Chief mechanic departments			+
Отдел главного энергетика Chief power engineer departments			+	Отделы главного конструктора Chief designer departments			+
Отдел маркетинга Marketing department	+			Главный инженер Chief engineer		+	
Финансово-экономический отдел Financial and economic department		+		Заместитель директора по производству Deputy director for production	+	+	
Отдел бухгалтерии Accounting department		+		Директор Director	+		
Заместитель директора по сбыту Deputy sales director	+			Главный экономист Chief economist	+		

В случае с ИАФ 2 – необходимости в регистрации техники не имеет смысла, т.к. все процессы происходят внутри одного здания. Политика большинства предприятий запрещает проносить персональную оргтехнику, т.е. появление сторонней незарегистрированной техники в них крайне маловероятна. Кроме того, внутренние связи, обеспечивающие критические процессы в целом не должны взаимодействовать со сторонней оргтехникой, от того и данного ИАФ – нет в перечислении.

ИАФ 7. Отказ от данной меры аналогично доводами из предыдущего пункта.

- УПД: 1-6, 9, 10, 13 ,15-17.

УПД 7 – информирование о наличии в ИС систем ИБ – неоправданно. Причина кроется в том, что при поступлении на работу на промышленных предприятиях практически всегда имеется документ, в котором разъясняются вопросы политики ИБ. Более того, сотрудники в обязательном порядке подписывают у руководителя документы соответствующего характера и, как правило, на начальника возлагается ответственность по доведению информации по данному вопросу до работников.

УПД 8 – на промышленных предприятиях за каждым сотрудником зарегистрирован свой АРМ, в кабинетах постоянно находятся несколько сотрудников, т.о. вероятность занятия АРМ сторонним сотрудником минимален.

УПД 11 – без идентификации пользователь не может попасть на сервер ИС. Как правило, нормы рассматриваемых копаний запрещают хранить коммерческие данные вне сервера, что соответствует политике ИБ, а, следовательно, в ограничении пользователей подобным образом нет смысла.

УПД 12 – метки безопасности неприменимы при рассмотрении только коммерческой тайны, т.к. это единственный уровень секретности.

УПД 14 неприменимо вследствие практически повсеместного использования проводных технологий связи. Это оправдано как с точки зрения обеспечения ИБ, так и с точки зрения скорости передачи данных что крайне важно в непрерывных техпроцессах, по большей части свойственных для промышленных предприятий.

– ОПС: 1-3.

Причиной не выбора ОПС 4 является тот факт, что достаточно много программ работают с оперативной памятью. Особенно это касается микроконтроллеров оборудования. В связи с необходимостью обеспечения быстроты техпроцесса, очистка может привести к простоям и сбиванию производственных циклов.

– ЗНИ: 1-4, 6-8.

ЗНИ 5 не оправдано применять на промышленном предприятии по причине повсеместного использования описанных в пункте средств для нужд. Кроме того, немаловажную роль играет отсутствие практической возможности вынести особо значимые материалы с большинства промышленных предприятий.

– РСБ: 1-8, АВЗ: 1,2, СОВ: 1, 2, АНЗ: 1-5, ЗСВ: 1-10.

Все элементы данных пунктов рационально применять на промышленном предприятии, потому разбирать исключения нет возможности.

– ОЦЛ: 1-3, 5, 6, 8.

ОЦЛ 4 нерационально применять, т.к. ИС промышленного предприятия по большей части создают с учетом отсутствия возможности выхода в сеть, соответственно и поступления писем в контура АС и средств обеспечения их должного функционирования невозможно.

ОЦЛ 7 неприменим в ИС промышленного предприятия, т.к. многие технические данные (большая часть информации) физически не могут быть оценены.

– ОДТ: 1, 3-6.

ОДТ 2 – для обеспечения коммерческой тайны использовать дублем дорогие технические средства защиты неоправданная роскошь, которую многие не смогут экономически позволить, потому данный пункт не стоит включать.

ОДТ 7 не оправдан на промышленном предприятии вследствие отсутствия необходимости в данном виде контроля.

– ЗТС: 2-5.

Коммерческая информация, обрабатываемая на промышленном предприятии крайне маловероятно будет считана через технические каналы вследствие потребности в использовании достаточно сложных и дорогих технических решений. Окупаемость таких процедур очень мала.

– ЗИС: 1, 3, 10, 20, 22, 26

ЗИС 2 – для промышленного предприятия то, что рассматривается в Методическом документе как низкоприоритетные процессы становятся куда значимее, из-за финансовой составляющей, потому и контроль над их исполнением бессмысленен.

Остальные ЗИС не были выбраны по причинам уже описанным выше; отмеченные ЗИСы дополняют их или тесно с ними связаны, как пример реализация мобильной технологии или процессов, явно замедляющих техпроцессы / засоряющих полосу пропускания, поэтому и их реализация неактуальна.

Комбинация отмеченных технологий ИБ формирует необходимую модель ЗИ коммерческих потоков на промышленном предприятии.

Вывод. Данное научное исследование может быть актуально как специалистам в области защиты информации, так и научным сотрудникам, занятым в области исследования обеспечения ИБ на промышленных предприятиях при обеспечении сохранности коммерческой тайны. Полученные в работе выкладки позволяют оценить динамику роста ущерба от КА, тем самым доказывая важность подобных исследований. Результаты исследования дают обоснование неоправданности применения некоторых мер при рассмотрении производства с точки зрения ЗИ коммерческого назначения.

Библиографический список:

1. Коновалова Г.И. Технология моделирования информационного процесса промышленного предприятия. Известия ТулГУ. Экономические и юридические науки. – 2012. – № 2(1). – С. 143-150
2. Ромашкина Н.Ю. Влияние глобальной компьютеризации на развитие экономической преступности в сфере компьютерной информации. Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики : сборник материалов III Всероссийской научно-практической конференции молодых ученых, Москва, 11 июня 2020 года, Москва: Московский университет МВД России имени В.Я. Кикотя. – 2020. – С. 588-591
3. Малышева, АА., Гусева ЕА., Ювченко ДА. Игровое моделирование стратегии защиты корпоративной сети предприятия от атак вредоносного программного обеспечения. Поколение будущего: взгляд молодых ученых - 2020 : сборник научных статей 9-й Международной молодежной научной конференции, Курск, 12–13 ноября 2020 года. Том 4, Курск: Юго-Западный государственный университет. – 2020. – С. 69-72
4. Лоскутов И.А. Общая характеристика информационной безопасности Российской Федерации. Молодёжный вестник Новороссийского филиала Белгородского государственного технологического университета им. В.Г. Шухова. – 2023. – № 3(2). – С. 168–174.
5. ISACA’s CYBERSECURITY NEXUS**.** [Электронный ресурс]. – URL: http://new.groteck.ru/images/catalog/39049/5818630bf28bcbd9a93f676aa7169fae.pdf (дата обращения 05.11.2024)
6. Банк данных угроз безопасности информации**.** [Электронный ресурс]. – URL: https://bdu.fstec.ru/ (дата обращения 01.10.2024).
7. Батаева И.П. Защита информации и информационная безопасность. Труды международного симпозиума «Надежность и качество». – 2012. – № 1. – С. 116-118.
8. Кибератаки на российские компании в I квартале 2023 года**.** [Электронный ресурс]. – URL: https://rt-solar.ru/upload/iblock/ad3/3j9s24qws3lcnjmoilaowut9afff7jco/Otchet-Kiberataki-na-rossiyskie-kompanii-v-I-kvartale-2023-goda.pdf (дата обращения 08.12.2024).
9. Количество действующих предприятий в России, по отраслям**.** [Электронный ресурс]. – URL: https://topic.ru/statistics/ekonomics-and-politic/business/kolichestvo-deystvuyushchikh-predpriyatiy-v-rossii-po-otraslyam/ (дата обращения 08.12.2024).
10. Мартынюк МС. Организационно-управленческие механизмы обеспечения кибербезопасности российских компаний. Финансовые рынки и банки. – 2023. – №6. – С. 5-9.
11. Актуальные киберугрозы для промышленных организаций: итоги 2022 года**.** [Электронный ресурс]. – URL: https://ict.moscow/research/aktualnye-kiberugrozy-dlia-promyshlennykh-organizatsii-itogi-2022-goda/ (дата обращения 15.12.2024).
12. Потери российских компаний от хакеров за год превысили десятки миллионов рублей**.** [Электронный ресурс]. – URL: https://www.ferra.ru/news/v-rossii/poteri-rossiiskikh-kompanii-ot-khakerov-za-god-prevysili-desyatki-millionov-rublei-06-09-2023.htm?ysclid=log9ja8fp0861142303 (дата обращения 20.12.2024).
13. Усачев СИ, Алиев ТФ. Киберпреступность: современное состояние и актуальные способы противодействия. Искусство правоведения. The art of law. – 2023. – № 1(5). – С. 75-59.
14. Базаров РТ., Хузина ГИ. Проблемы обеспечения экономической безопасности на предприятии: киберпреступления. Вестник Университета управления "ТИСБИ". – 2022. – № 3. – С. 15-25.
15. Шаломов НС. Экономические проблемы модернизации оборудования на предприятиях. Инновационная наука. – 2022. – № 6(1). – С. 87-89.

References:

1. Konovalova G.I. Technology of modeling the information process of an industrial enterprise. News of Tula State University. *Economic and legal sciences*. 2012;2(1):143-150. (In Russ)

2. Romashkina N.Yu. The impact of global computerization on the development of economic crime in the field of computer information. Issues of improving law enforcement: the interaction of science, rule-making and practice: collection of materials from the III All-Russian scientific and practical conference of young scientists, Moscow, June 11, 2020, Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. 2020;588-591(In Russ)

3. Malysheva, AA, Guseva EA, Yuvchenko DA. Game modeling of the strategy for protecting the corporate network of an enterprise from malware attacks. Generation of the Future: a View of Young Scientists - 2020: Collection of Scientific Articles of the 9th International Youth Scientific Conference, Kursk, November 12-13, 2020. Vol. 4, Kursk: South-West State University. 2020; 69-72(In Russ)

4. Loskutov I.A. General Characteristics of Information Security of the Russian Federation. *Youth Bulletin of the Novorossiysk Branch of the Belgorod State Technological University named after V.G. Shukhov*. 2023;3 (2):168-174. (In Russ)

5.ISACA's CYBERSECURITY NEXUS. [Electronic resource]. – URL: http://new.groteck.ru/images/catalog/39049/5818630bf28bcbd9a93f676aa7169fae.pdf (date of access 05.11.2024)

6. Database of information security threats. [Electronic resource]. – URL: https://bdu.fstec.ru/ (date of access 01.10.2024). (In Russ)

7. Bataeva I.P. Information protection and information security. *Proceedings of the international symposium "Reliability and quality"*. 2012;1:116-118. (In Russ)

8. Cyberattacks on Russian companies in the first quarter of 2023. [Electronic resource]. – URL: https://rt-solar.ru/upload/iblock/ad3/3j9s24qws3lcnjmoilaowut9afff7jco/Otchet-Kiberataki-na-rossiyskie-kompanii-v-I-kvartale-2023-goda.pdf (date of access 08.12.2024). (In Russ)

9. Number of operating enterprises in Russia, by industry. [Electronic resource]. – URL: https://topic.ru/statistics/ekonomics-and-politic/business/kolichestvo-deystvuyushchikh-predpriyatiy-v-rossii-po-otraslyam/ (date of access 08.12.2024). (In Russ)

10. Martynyuk MS. Organizational and managerial mechanisms for ensuring cybersecurity of Russian companies. *Financial markets and banks*. 2023;6:5-9. (In Russ)

11. Current cyber threats to industrial organizations: results of 2022. [Electronic resource]. – URL: https://ict.moscow/research/aktualnye-kiberugrozy-dlia-promyshlennykh-organizatsii-itogi-2022-goda/ (date of access 12/15/2024). (In Russ)

12. Losses of Russian companies from hackers in a year exceeded tens of millions of rubles. [Electronic resource]. – URL: https://www.ferra.ru/news/v-rossii/poteri-rossiiskikh-kompanii-ot-khakerov-za-god-prevysili-desyatki-millionov-rublei-06-09-2023.htm?ysclid=log9ja8fp0861142303 (date of access 20.12.2024). (In Russ)

13. Usachev S.I,. Aliev T.F. Cybercrime: current state and current methods of counteraction. *The art of law*. 2023;1(5):75-59. (In Russ)

14. Bazarov RT., Khuzina GI. Problems of ensuring economic security at the enterprise: cybercrime. *Bulletin of the University of Management "TISBI"*. 2022;3:15-25. (In Russ)

15. Shalomov N.S. Economic problems of equipment modernization at enterprises. *Innovative science*. 2022;6(1): 87-89. (In Russ)

Сведения об авторах:

Иван Андреевич Лоскутов, инженер – конструктор, отдел 55; преподаватель; младший научный сотрудник; faxvex@ya.ru

Сергей Евгеньевич Акатов**,** ведущий инженер; akatov.serg@gmail.com

Information about the authors:

Ivan A. Loskutov, Engineer-constructor, Department 55, faxvex@ya.ru

Sergey E. Akatov, Lead Engineer; akatov.serg@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 20.12.2024.

Одобрена после рецензирования / Reviced 20.01.2025.

Принята в печать /Accepted for publication 20.05.2025.