Publishing House "ANALITIKA RODIS" (analitikarodis@yandex.ru) http://publishing-vak.ru/

УДК 004.0 **DOI: 10.34670/AR.2026.15.37.019**

Инциденты, связанные с информационной безопасностью, и использование средств защиты информации в организациях промышленного сектора России

Иосип Игорь Викторович

ООО НТЦ «БИНАРТЕЛЕКОМ»,
119021, Российская Федерация, Москва, переулок Оболенский, 10, стр. 1;
e-mail: 7290916@mail.ru

Аннотация

Настоящая работа посвящена статистическому анализу двух направлений информационной безопасности в организациях промышленного сектора по данным опросов Росстата. Первое направление — это исследование статистики связанных с информационной безопасностью инцидентов в 2024 г. Второе направление оценивает использование промышленными организациями России различных средств защиты информации за 2024 г. В ходе работы установлено, что наилучшие результаты в области информационной безопасности наблюдаются в более финансово обеспеченных направлениях: в нефте- и газодобыче, в производстве нефти и нефтепродуктов, а также в электронной промышленности. Во многом массовость отрицательного воздействия инцидентов, связанных с информационной безопасностью, обусловлена относительно невысокой степенью использования различных информационных средств защиты: в среднем по промышленному сектору уровенб использования различных средств немногим превышает 53%. Чуть выше он для предприятий топливного сектора, производства кокса и нефтепродуктов, лекарственных средств, табачных изделий. Самый низкий уровень использования информационных средств защиты в секторе водоснабжения, водоотведения и обращения с отходами (43%), что обуславливает высокую степень отрицательных последствий различных инцидентов, связанных с цифровой безопасностью.

Для цитирования в научных исследованиях

Иосип И.В. Инциденты, связанные с информационной безопасностью, и использование средств защиты информации в организациях промышленного сектора России // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 5А. С. 194-204. DOI: 10.34670/AR.2026.15.37.019

Ключевые слова

Информационная безопасность, инциденты, средства защиты данных, статистика, цифровизация, методология исследования.

Введение

Повсеместная цифровизация всех сфер социально-экономической деятельности является объективным следствием технологического прогресса, и внедрение цифровых технологий является в настоящее время определяющим фактором не только конкурентоспособности предприятия, отрасли или экономики в целом, но даже больше – фактически неотъемлемым атрибутом. Практически невозможно представить большинство процессов без непосредственного или сопутствующего применения цифровых технологий. Однако, цифровая трансформация аккумулирует в себе и значительные риски как технологического, так и социального характера [Никандров, 2021; Смотрова, Шендрикова, 2025]. Риски, связанные, в том числе, с опасностью утечки данных, нарушением технологических и управленческих процессов, управляемых или сопровождаемых цифровыми средствами и технологиями [Гладилин, 2024; Кошелев, 2021].

Цель исследования. Рассмотреть инциденты, связанные с информационной безопасностью, и использование средств защиты информации в организациях различных отраслей промышленности России. Объектом исследования выступают отрасли промышленности РФ, их устойчивость и эффективность. Предметом исследования являются экономические последствия киберинцидентов и эффективность затрат на информационную безопасность в отраслевом разрезе.

В этом контексте стоит привести данные опросов Росстата за 2022 г. (более поздние данные опросов по оценке степени влияния отсутствуют) касательно эффектов внедрения различных цифровых технологий, в том числе в контексте их влияния на безопасность труда (таблица 1).

Таблица 1 - Доля организаций промышленного сектора, оценивших степень влияния внедрения отдельных цифровых технологий на безопасность труда работников, %

Наименование	Оценка влияния		
	отрицательное	не повлияло	положительное
Технологии сбора, обработки и анализа больших данных	12	80	8
Технологии искусственного интеллекта	3	90	8
Интернет вещей	2	81	17
Другие цифровые технологии	2	73	25

Источник: рассчитано по данным Росстата [Росстат, 2024]

Как видно из таблицы 1, внедрение цифровых технологий оказывает достаточно противоречивое воздействие на такую сторону деятельности организаций, как безопасность труда работников. Вероятнее всего, это связано с возможным отрицательным влиянием на безопасность личных данных. Хорошо заметно, что по оценкам самих организаций промышленной сферы внедрение Big Data скорее оказалось отрицательным, чем положительным по эффекту, оказанному на уровень безопасности труда. Очевидно, в связи с вероятными или фактическими утечками информации, в том числе личной. В остальных же направлениях положительный эффект в среднем оказался выше отрицательного. Хотя, по большому счёту, основная часть технологий не оказывает в принципе никакого воздействия на безопасность труда сотрудников. Ещё раз стоит подчеркнуть, что в данном случае речь идёт не об эффективности цифровых технологий, а лишь о степени влияния на узкий аспект деятельности опрашиваемых организаций.

Материалы и методы исследования

Таким образом, можно подытожить, что внедрение цифровых технологий, по сути, представляет собой некий баланс между конкурентоспособностью и рисками функционирования, где обе стороны влияют на способность организации, отрасли или экономики к развитию, что нашло отражение в работах ряда исследователей: Лосевой А.В. [Лосева, Леднева, 2021], Морозовой Г.А. [Морозова, Лапаев, 2019], Никандрова М.В. [Никандров, Селезнев, 2019], Одинцова В.О. [Одинцов, 2023], Ратниковой Е.А. [Ратникова, Щеулина, 2022], Савушкина М.Ю. [Савушкин, Мокрушин, Жуков, 2020]. Актуальность проблематики вызывает повышенный профессиональный интерес в научной среде к проблематике снижения рисков преднамеренных воздействий на деятельность организаций, использующих цифровые технологии.

В целом перечисленные авторы склоняются к однозначному мнению о растущей важности принятия во внимание вопросов, связанных с информационной безопасностью, поскольку выгоды от использования технологий неизбежно сопровождаются рисками, что частично нашло отражение в таблице 1. Однако, в указанных выше работах не представлены статистические данные, которые могли бы иллюстрировать динамику или текущую ситуацию в этом вопросе. Настоящее исследование призвано проанализировать текущий прогресс в области кибербезопасности и использовании средств защиты информации в организациях промышленного сектора страны и обозначить некоторые статистические величины в данной области.

Результаты и обсуждение

Структурно исследование разделено на два основных направления:

– оценка количества инцидентов в организациях промышленного сектора России в области информационной безопасности за 2024 г.;

– оценка применяемых в организациях промышленного сектора России средств защиты информации на 2024 г.

К инцидентам в области информационной безопасности относятся события, которые приводят к полной или частичной утрате данных, а также к их «утечкам»; либо события, приводящие к сбоям, полной или частичной утрате работоспособности различных ресурсов или оборудования. Это могут быть фишинговые атаки, несанкционированный доступ, заражение вредоносным программным обеспечением и т.д. В текущем исследовании все указанные события группируются и анализируются с позиции нанесённого ими ущерба.

В обозначенном контексте ситуацию с кибербезопасностью характеризуют следующие статистические данные: в 2024 г. по информации опросов Росстата [Росстат, 2024] 42,6 тыс. российских организаций столкнулись с инцидентами, связанными с заражением вредоносными программами, компьютерными атаками и в целом несанкционированным вторжением на собственные ресурсы и оборудование. Из них почти 5,5 тыс. организаций относятся к промышленной отрасли. Данные по ним в разрезе кодов ОКВЭД2 за 2024 г. приведены в таблице 2. Стоит отметить, что, не смотря на то, что в ряде случаев по отдельным направлениям экономической деятельности охват предприятий оказался не очень большим (порядка нескольких десятков предприятий), тем не менее, для целей текущего исследования выборка представляется репрезентативной.

Таблица 2 - Организации промышленного сектора, столкнувшиеся с инцидентами, связанными с различными нарушениями информационной безопасности в 2024 г., единиц/%

Код ОКВЭД2	Число организаций, единиц	Интенсивность последствий*	в том числе, %		
			блокирование ресурсов/ оборудования, сбои в работе	«утечки» данных	потеря данных
Всего по всем отраслям экономики					
всего	42631	65	29	16	20
Промышленный сектор					
всего	5450	59	27	13	20
B	475	55	23	13	18
05	56	39	16	13	11
06	71	14	6	3	6
07	65	48	22	12	14
08	78	96	38	24	33
09	205	59	26	14	20
C	3725	60	28	12	20
10	601	64	30	12	22
11	116	110	41	33	36
13	77	83	26	9	48
14	48	92	38	23	31
15	17	118	41	29	47
16	84	65	31	12	23
17	77	64	27	16	21
18	40	85	28	25	33
19	56	30	23	4	4
20	232	56	34	8	13
21	81	36	16	7	12
22	206	56	25	14	18
23	266	62	32	9	21
24	134	46	21	13	13
25	316	66	34	12	20
26	209	26	12	6	8
27	172	51	24	11	16
28	259	53	23	12	19
29	140	44	19	7	19
30	119	34	17	5	13
31	67	79	30	19	30
32	101	167	61	50	55
33	303	45	31	6	8
D	823	43	18	10	15
35	823	43	18	10	15
E	427	86	35	22	29

Примечание: сумма долей предприятий, столкнувшихся с инцидентами в области информационной безопасности. Последствия разделены на 3 категории, и конечный показатель «интенсивность последствий» является суммой этих долей. Показатель может быть более 100% из-за того, что злонамеренные действия могут иметь различные негативные последствия (арифметически: сумма столбцов «блокирование ресурсов/ оборудования, сбои в работе», «утечки» данных и «потеря данных»). Источник: рассчитано по данным Росстата [Росстат, 2024]

В целом в промышленности интенсивность последствий, составила 59% против 65% в целом по экономике, что свидетельствует о чуть большем развитии средств цифровой безопасности в

промышленном секторе. Как видно из таблицы 2, на первом месте среди последствий информационных инцидентов (далее в статье – инциденты) в области безопасности в 2024 г. оказалось блокирование или сбои в работе информационных ресурсов и оборудования промышленных предприятий. На них пришлось 29% имеющих последствия событий. 20% инцидентов связаны с полной или частичной потерей данных, а 16% – с их утечкой. То есть, основным риском информационной безопасности практически для всех организаций является выход из строя/блокирование/сбои ресурсов или оборудования.

Для добычи полезных ископаемых (код ОКВЭД «B») показатель интенсивности последствий составит 55%. Для обрабатывающего сектора (код «C») он составит 60%, для электроэнергетики (код «D») – 43%, для сектора водоснабжения и деятельности по обращению с отходами (код «E») – 86%. Можно заметить, что последний вид экономической деятельности в плане информационной безопасности находится в наиболее уязвимом положении. Самая же положительная статистика наблюдается для энергетики.

В разрезе отдельных видов экономической деятельности наибольший ущерб (в выражении показателя интенсивности последствий) наблюдается в отрасли производства прочих готовых изделий (код ОКВЭД «32»). Здесь в 61% случаев инциденты привели к блокировке или сбою в работе ресурсов предприятий, в 55% к потере данных, в 50% – к их утечке. То есть, по большому счёту, либо все злонамеренные атаки могли быть успешными с точки зрения их выгодоприобретателей, либо имели два и более последствий. Схожая ситуация наблюдается в производствах напитков (код «11») и в кожевенной отрасли (код «15»). Здесь, очевидно, ситуация с цифровой безопасностью находится в наихудшей ситуации. Также достаточно высокими являются отрицательные последствия для лёгкой промышленности в целом (коды с «13 по «15») и добычи прочих полезных ископаемых (код «08»).

При этом наименьший показатель интенсивности последствий имели информационные инциденты в секторах добычи нефти и природного газа (всего 14%), угля (39%), электронной промышленности (26%), производства кокса и нефтепродуктов (30%), производствах прочих транспортных средств (34%).

То есть, можно сделать достаточно логичный вывод, что чем менее финансово обеспеченной является отрасль, тем с большими потерями и рисками в плане информационной безопасности она сталкивается вследствие различных инцидентов. Так, как можно заключить из анализа таблицы 2, наилучшие результаты в области информационной безопасности имеет сектор нефте- и газодобычи. Худшие – лёгкая промышленность, производства прочих готовых изделий и напитков.

Данные по использованию различных средств информационной защиты организациями промышленности России сведены в таблицу 3. Стоит отметить, что данные таблицы 3 характеризуют лишь количественные параметры использования того или иного программного обеспечения вне контекста его качественных характеристик.

Как можно отметить из анализа таблицы 3, в среднем применение всех 9 основных групп информационных средств защиты составляет порядка 50% для всех направлений экономики в целом и в частности для организаций промышленности около 53%. Чаще всего используются средства строгой аутентификации (79% использующих такие технологии организаций по промышленному сектору), брандмауэры (74%) и спам-фильтры (70%). Реже всего применяются биометрические средства аутентификации пользователей (8% организаций).

Наибольшая средняя доля применений всех видов средств информационно защиты наблюдается для добычи угля и нефти (62%), производства напитков (65%), табака и табачных

изделий (69%), кокса и нефтепродуктов (69%) и лекарственных средств (64%). Менее 50% организаций в среднем применяют средства информационной защиты в отраслях производства одежды (50%), деревообработки (49%), текстильной (48%) и кожевенной (46%). Можно снова наблюдать некоторую зависимость доли применений средств информационной безопасности от финансовой обеспеченности отрасли: в лёгкой промышленности такая доля ощутимо ниже. Лидерами же снова являются нефтепереработка, добыча нефти, газа и угля.

Таблица 3 - Доля организаций, использовавших различные информационные средства защиты в 2024 г., %

Код ОКВЭД2	Всего организаций, единиц	из них доля использовавших, %								
		Средства шифрования	VPN	Средства строгой аутентификации	Резервное копирование данных	Биометрию	Брандмауэр	Спам-фильтр	Системы обнаружения вторжения	Средства анализа и контроля защищенности компьютерных систем
Всего по всем отраслям экономики										
всего	203933	63	44	79	39	9	67	63	52	46
Промышленный сектор										
всего	23356	62	48	79	40	8	74	70	55	45
B	2126	63	56	83	42	7	78	73	59	50
05	175	71	62	86	46	13	86	79	63	49
06	334	69	63	88	33	6	85	78	68	63
07	283	65	54	82	39	3	77	67	57	49
08	346	60	42	75	42	8	68	66	53	39
09	988	59	58	84	45	6	78	75	57	49
C	15589	62	51	79	42	9	76	72	57	45
10	2534	57	51	76	42	9	73	68	54	41
11	563	74	69	88	46	12	76	84	74	62
12	26	73	77	85	69	23	92	77	65	58
13	242	52	37	78	37	7	79	71	41	31
14	247	61	47	77	39	5	64	57	53	48
15	70	50	33	74	34	6	77	54	47	36
16	387	57	34	79	47	6	66	64	51	39
17	309	61	50	77	41	9	82	75	60	52
18	200	55	34	65	43	7	64	67	53	46
19	173	79	71	92	53	12	88	86	77	67
20	952	65	54	76	43	10	75	71	55	47
21	345	74	68	86	58	7	85	83	74	43
22	813	54	43	72	43	9	72	65	52	44
23	1159	63	52	80	46	8	76	69	56	41
24	578	70	55	81	46	7	79	75	60	51
25	1354	64	45	77	40	9	74	70	56	49
26	946	61	50	84	37	9	84	81	62	45
27	727	61	53	79	42	9	80	77	57	42
28	1038	59	47	78	39	8	78	73	56	42

Код ОКВЭД2	Всего организаций, единиц	из них доля использовавших, %								
		Средства шифрования	VPN	Средства строгой аутентификации	Резервное копирование данных	Биометрию	Брандмауэр	Спам-фильтр	Системы обнаружения вторжения	Средства анализа и контроля защищенности компьютерных систем
29	495	63	53	83	38	9	78	70	58	45
30	541	64	61	85	32	5	82	74	56	46
31	216	59	48	71	44	12	65	72	51	39
32	355	59	56	73	53	23	74	68	55	46
33	1319	62	47	85	35	5	76	73	57	47
D	3643	66	43	80	35	6	74	67	55	43
E	1998	58	33	69	35	5	55	52	40	37

Источник: рассчитано по данным Росстата [Росстат, 2024]

Таблица 4 характеризует экономическую сторону вопроса обеспечения информационной защиты предприятий промышленного сектора. В таблице 4 оценивается доля затрат на информационную безопасность в общих затратах на внедрение и поддержку использования цифровых технологий предприятиями.

Таблица 4 - Показатели, характеризующие информационную безопасность (ИБ) и финансовые результаты организаций в 2024 г., %

Код ОКВЭД2	Доля расходов на ИБ, %	Расход на 1 организацию в области ИБ, тыс. руб.	Сальдо финансового результата организаций, млрд руб.	Прибыль организаций, млрд руб.	Интенсивность последствий
Сокращение	X1	X2	X3	X4	Y
05	1,0	33	-113	140	39
06	6,8	25951	5275	5657	14
07	4,0	1068	1169	1232	48
08	0,5	171	44	116	96
10	1,8	24	771	828	64
11	2,4	50	165	179	110
12	0,3	17	138	139	83
13	2,0	569	36	37	92
14	2,1	146	49	50	118
15	1,2	21	4	7	65
16	1,4	573	24	88	64
17	1,4	200	185	195	85
18	6,5	288	51	53	30
19	10,4	35880	2782	2934	56
20	4,3	9202	1013	1231	36
21	1,0	82	263	274	56
22	1,4	243	180	189	62

Код ОКВЭД2	Доля расходов на ИБ, %	Расход на 1 организацию в области ИБ, тыс. руб.	Сальдо финансового результата организаций, млрд руб.	Прибыль организаций, млрд руб.	Интенсивность последствий
Сокращение	**X1**	**X2**	**X3**	**X4**	**Y**
23	4,0	358	326	359	46
24	4,2	1804	1711	1845	66
25	2,1	2287	520	565	26
26	2,1	799	392	426	51
27	1,5	217	232	245	53
28	2,2	761	286	319	44
29	7,1	1379	186	221	34
30	3,6	3586	253	378	79
31	0,6	24	21	23	167
32	1,4	149	35	38	45
D	7,1	6747	1056	1425	43
E	6,6	202	108	153	86

Источник: рассчитано по данным Росстата [Росстат, 2024].

Как видно из таблицы 4, максимальный уровень расходов в области информационной безопасности в расчёте на 1 организацию, а также в относительном выражении доли расходов на ИБ в общем объёме затрат на цифровые технологии наблюдается в нефтегазовом секторе, а также производстве кокса и нефтепродуктов. То есть, топливная промышленность располагает максимальными ресурсами для обеспечения собственной цифровой безопасности в сравнении с остальными экономическим направлениями.

Если рассчитать корреляцию показателей X1-Y и X2-Y (сокращения – см. наименования столбцов в таблице 4), то коэффициенты корреляции для таких моделей составят значения 0,40 и 0,28 соответственно при уровне статистической значимости 0,03 и 0,12. Из этих данных можно сделать вывод о наличии обратной зависимости между долей расходов на информационную безопасность и фактической долей инцидентов, имеющих отрицательные последствия (уравнение принимает вид $Y = 79{,}22 – 4{,}97*X1$). И чем выше доля затрат в отдельных отраслях на ИБ, тем ниже интенсивность инцидентов, связанных с различными нарушениями информационной безопасности.

Добавление в анализ показателей финансового состояния организаций отраслей (переменные X3 и X4) демонстрирует достаточно высокую степень зависимости доли расходов на ИБ (X1) от показателей финансовой устойчивости отраслей (X3 и X4). Коэффициенты корреляции моделей X1-X3 и X1-X4 в обоих случаях составляют 0,58 при уровне статистической значимости 0,001. Это говорит о высокой степени зависимости уровня расходов на ИБ от абсолютного значения прибыли и сальдо прибылей и убытков, причём стоит обратить внимание на то, что уровень расходов в данном случае выражен в относительных величинах. Следовательно, экономический фактор является определяющим в возможностях организаций в обеспечении собственной информационной безопасности.

Причём нельзя сказать, что экспортная ориентация отрасли играет существенную роль: например, экспортоориентированные отрасли добычи угля или металлургия демонстрируют долю расходов на ИБ на уровне среднего или ниже. А именно эти направления в последние годы столкнулись с ухудшением экономического положения. Возвращаясь к моделям X1-X3 и X1-X4, можно заметить логичность демонстрируемого ими результата – именно экономика, а не

иные факторы играют определяющую роль в расходах организаций на ИБ. Что, в свою очередь, оказывает прямое влияние на интенсивность последствий (модель X1-Y).

Заключение

В целом по суммарному анализу таблиц 1-4 можно отметить зависимость уровня информационной безопасности, последствий различных цифровых инцидентов и доли использующих те или иные программные решения в области компьютерной безопасности от отраслевого направления. Максимальная доля используемого программного обеспечения и самые низкие показатели отрицательных последствий инцидентов наблюдаются в секторах, связанных с добычей и переработкой нефти и газа. Напротив, самые худшие показатели наблюдаются для текстильной отрасли, в секторе водоснабжения, водоотведения и обращения с отходами и отчасти в деревообработке, уровень финансовой обеспеченности и общего отраслевого развития которых фактически несоизмерим с нефтегазовым сектором.

В экономическом отношении имеет значение доля затрат предприятий на информационную безопасность – чем выше этот показатель, тем ниже доля инцидентов, связанных с различными нарушениями информационной безопасности. Таким образом, действующим фактором является, прежде всего, экономика: системное недоинвестирование информационной устойчивости ожидаемо ведёт к ухудшению информационной безопасности в отраслевом выражении.

Экономический фактор, как следствие, находит прямое отражение в статистике использования средств защиты информации: в целом использование отдельных элементов системы информационной безопасности значительно шире применяется именно в секторах, связанных с добычей и переработкой нефти и газа. Минимальная же доля использований отдельных видов средств информационной защиты наблюдается в лёгкой промышленности, предприятия которой обладают заведомо меньшими финансовыми возможностями. Нельзя сказать, что рост затрат на информационную безопасность обусловлен вероятностью интенсивности последствий или более выражен в информационно-зависимых отраслях – здесь сказывается исключительно фактор финансовых возможностей предприятий отрасли.

Библиография

1. Гладилин А.К. Особенности цифровизации предприятий оборонной промышленности // Вестник евразийской науки. 2024. Т. 16. № S5. URL: https://elibrary.ru/download/elibrary_80383807_76462838.pdf .
2. Кошелев А.Д. Обеспечение информационной безопасности предприятия в условиях массовой цифровизации // Экономика: вчера, сегодня, завтра. 2021. Т. 11, № 10-1. С. 287–295. DOI: 10.34670/AR.2021.92.59.033.
3. Лосева А.В., Леднева О.В. Вопросы территориальной дифференциации информационного общества России // Фундаментальные исследования. 2021. № 6. С. 47–55. DOI: 10.17513/fr.43057.
4. Морозова Г.А., Лапаев Д.Н. Современная цифровизация и обеспечение безопасности // Развитие и безопасность. 2019. № 1. С. 70–81. DOI: 10.46960/74159_2019_1_70.
5. Наука, инновации и технологии: сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг (итоги статнаблюдения по ф. № 3-информ) // Росстат. URL: https://rosstat.gov.ru/statistics/science .
6. Никандров М.В., Селезнев М.И. Аспекты обеспечения информационной безопасности локально-вычислительных сетей цифровых подстанций // Релейщик. 2019. № 2(34). С. 44–46.
7. Никандров Н.Д. Цифровизация: потенциал, достижения, риски // Мир психологии. 2021. № 1-2(105). С. 75–88.
8. Одинцов В.О. Экономическая безопасность кредитных организаций в условиях роста цифровых рисков // Вестник евразийской науки. 2023. Т. 15, № 6. DOI: 10.15862/64ecvn623.
9. Ратникова Е.А., Щеулина Т.В. Влияние рисков цифровизации на конкурентоспособность высокотехнологичных предприятий авиастроительной отрасли // Вестник Академии знаний. 2022. № 48(1). С. 267–276. DOI:

10.24412/2304-6139-2022-48-1-267-277.
10. Савушкин М.Ю., Мокрушин П.Г., Жуков Д.М. Вызовы цифровой экономики // Сила систем. 2020. № 3(16). С. 37–43.
11. Смотрова Т.И., Шендрикова О.О. Обеспечение экономической безопасности предприятия в условиях цифровой трансформации // Экономинфо. 2025. Т. 20, № 2. С. 13–21.
12. Финансовые результаты деятельности организаций в 2024 году // Росстат. URL: https://rosstat.gov.ru/storage/mediabank/30_05-03-2025.html .

Information Security Incidents and the Use of Information Protection Tools in Organizations of the Industrial Sector of Russia

Igor' V. Iosip

STC "BINARTELECOM" LLC,
119021, 10, bld. 1, Obolenskiy lane, Moscow, Russian Federation;
e-mail: 7290916@mail.ru

Abstract

This work is devoted to the statistical analysis of two areas of information security in organizations of the industrial sector based on Rosstat survey data. The first area is the study of statistics of information security-related incidents in 2024. The second area assesses the use of various information protection tools by Russian industrial organizations in 2024. In the course of the work, it has been established that the best results in the field of information security are observed in more financially secure areas: in oil and gas extraction, in the production of oil and petroleum products, as well as in the electronics industry. In many respects, the mass scale of the negative impact of information security-related incidents is due to the relatively low degree of use of various information protection tools: on average in the industrial sector, the level of use of various tools slightly exceeds 53%. It is slightly higher for enterprises in the fuel sector, the production of coke and petroleum products, medicines, and tobacco products. The lowest level of use of information protection tools is in the sector of water supply, wastewater disposal, and waste management (43%), which causes a high degree of negative consequences of various incidents related to digital security.

For citation

Iosip I.V. (2026) Intsidenty, svyazannye s informatsionnoy bezopasnost'yu, i ispol'zovanie sredstv zashchity informatsii v organizatsiyakh promyshlennogo sektora Rossii [Information Security Incidents and the Use of Information Protection Tools in Organizations of the Industrial Sector of Russia]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (5A), pp. 194-204. DOI: 10.34670/AR.2026.15.37.019

Keywords

Information security, incidents, data protection tools, statistics, digitalization, research methodology.

References

1. Financial performance of organizations in 2024. (2024). Rosstat. https://rosstat.gov.ru/storage/mediabank/30_05-03-2025.html

2. Gladilin, A. K. (2024). Osobennosti tsifrovizatsii predpriyatiy oboronnoy promyshlennosti [Features of digitalization of defense industry enterprises]. Vestnik evraziyskoy nauki [The Eurasian Scientific Journal], 16(S5). https://elibrary.ru/download/elibrary_80383807_76462838.pdf
3. Koshelev, A. D. (2021). Obespechenie informatsionnoy bezopasnosti predpriyatiya v usloviyakh massovoy tsifrovizatsii [Ensuring the information security of an enterprise in the context of mass digitalization]. Ekonomika: vchera, segodnya, zavtra [Economics: Yesterday, Today and Tomorrow], 11(10-1), 287–295. https://doi.org/10.34670/AR.2021.92.59.033
4. Loseva, A. V., & Ledneva, O. V. (2021). Voprosy territorial'noy differentsiatsii informatsionnogo obshchestva Rossii [Issues of territorial differentiation of the information society in Russia]. Fundamental'nye issledovaniya [Fundamental Research], 6, 47–55. https://doi.org/10.17513/fr.43057
5. Morozova, G. A., & Lapaev, D. N. (2019). Sovremennaya tsifrovizatsiya i obespechenie bezopasnosti [Modern digitalization and security]. Razvitie i bezopasnost' [Development and Security], 1, 70–81. https://doi.org/10.46960/74159_2019_1_70
6. Nikandrov, M. V., & Seleznev, M. I. (2019). Aspekty obespecheniya informatsionnoy bezopasnosti lokal'no-vychislitel'nykh setey tsifrovykh podstantsiy [Aspects of ensuring the information security of local area networks of digital substations]. Releyshchik, 2(34), 44–46.
7. Nikandrov, N. D. (2021). Tsifrovizatsiya: potentsial, dostizheniya, riski [Digitalization: Potential, achievements, risks]. Mir psikhologii [The World of Psychology], 1-2(105), 75–88.
8. Odintsov, V. O. (2023). Ekonomicheskaya bezopasnost' kreditnykh organizatsiy v usloviyakh rosta tsifrovykh riskov [Economic security of credit organizations amid growing digital risks]. Vestnik evraziyskoy nauki [The Eurasian Scientific Journal], 15(6). https://doi.org/10.15862/64ecvn623
9. Ratnikova, E. A., & Shcheulina, T. V. (2022). Vliyanie riskov tsifrovizatsii na konkurentosposobnost' vysoko-tekhnologicheskikh predpriyatiy aviastroitel'noy otrasli [The impact of digitalization risks on the competitiveness of high-tech enterprises in the aircraft manufacturing industry]. Vestnik Akademii znaniy [Bulletin of the Academy of Knowledge], 48(1), 267–276. https://doi.org/10.24412/2304-6139-2022-48-1-267-277
10. Rosstat. (2024). Nauka, innovatsii i tekhnologii: svedeniya ob ispol'zovanii tsifrovykh tekhnologiy i proizvodstve svyazannykh s nimi tovarov i uslug [Science, innovation and technology: Information on the use of digital technologies and the production of related goods and services]. https://rosstat.gov.ru/statistics/science
11. Savushkin, M. Yu., Mokrushin, P. G., & Zhukov, D. M. (2020). Vyzovy tsifrovoy ekonomiki [Challenges of the digital economy]. Sila sistem, 3(16), 37–43.
12. Smotrova, T. I., & Shendrikova, O. O. (2025). Obespechenie ekonomicheskoy bezopasnosti predpriyatiya v usloviyakh tsifrovoy transformatsii [Ensuring the economic security of an enterprise in the context of digital transformation]. Ekonominfo, 20(2), 13–21.