ГИАБ. Горный информационно-аналитический бюллетень /
MIAB. Mining Informational and Analytical Bulletin, 2022;(2):81-96
ОРИГИНАЛЬНАЯ СТАТЬЯ / ORIGINAL PAPER

УДК 004.056.53:65.011.56 DOI: 10.25018/0236_1493_2022_2_0_81

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ КОРПОРАТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

С.Н. Гончаренко[1], В.В. Яхеев[2]

[1] НИТУ «МИСиС», Москва, Россия, e-mail: gsn@misis.ru
[2] Санкт-Петербургский университет Государственной противопожарной службы МЧС России, Санкт-Петербург, Россия

Аннотация: Рассмотрены подходы к разработке эффективных управленческих решений по созданию комплексной системы управления информационной безопасностью геоинформационных технологий промышленного предприятия, необходимой для организации и контроля процесса защиты информации, и анализа рисков. Предложенные методы и модели оценки рисков информационной безопасности геоинформационных технологий позволяют определить единый подход к детализации ключевых рисков в области информационной безопасности, что означает рассмотрение ключевого риска в деталях, его конкретизацию в отдельных рисках, идентификацию и установление величины возможного ущерба, а также выбор необходимых мер по нейтрализации рисков в рамках системы управления информационной безопасностью геоинформационных технологий промышленного предприятия. С помощью приведенных методов и моделей идентифицируются угрозы для информационных активов и уязвимости их защиты, оценивается вероятность их реализации, а также возможное негативное воздействие на деятельность геоинформационных систем промышленного предприятия. Нейтрализация рисков информационной безопасности осуществляется путем воздействия на составляющие этих рисков, т.е. на соответствующие уязвимости, угрозы, активы или средства управления безопасностью. В результате исследований показаны основные эффекты от внедрения комплексной системы информационной безопасности геоинформационных технологий в сфере оперативного реагирования на инциденты: снижение комплексных затрат за счет тиражирования технологии и эффекта масштаба внедрения геоинформационных систем, повышение уровня информационной безопасности и снижение факторов риска, а также снижение ущерба от кибератак.

Ключевые слова: риски информационной безопасности геоинформационных технологий, оценка уязвимостей, оценка угроз, ценность информационного актива, средства управления информационной безопасностью геоинформационных технологий, оценивание и обработка риска, меры по нейтрализации рисков, защита информации в геоинформационных системах, ущерб от кибератак, оперативное реагирование на инциденты.

Для цитирования: *Гончаренко С. Н., Яхеев В. В.* Компьютерное моделирование корпоративной системы информационной безопасности геоинформационных технологий промышленного предприятия // Горный информационно-аналитический бюллетень. – 2022. – № 2. – С. 81–96. DOI: 10.25018/0236_1493_2022_2_0_81.

© С.Н. Гончаренко, В.В. Яхеев. 2022.

Computer modeling of corporate information security of geoinformation technologies at industrial facilities

S.N. Goncharenko[1], V.V. Yakheev[2]

[1] National University of Science and Technology «MISiS», Moscow, Russia, e-mail: gsn@misis.ru
[2] Saint-Petersburg University of State Fire Service of Emercom of Russia, Saint-Petersburg, Russia

Abstract: The article discusses approaches to efficient managerial decision-making in integrated information security of geoinformation technologies in industry, which is required for the information protection organization and control, and for the risk assessment. The proposed methods and models of risk assessment in information security of geoinformation technologies make it possible to identify a unified approach to specification of key risks in information security. This means that a key risk is scrutinized and fleshed out, a possible damage is identified and evaluated, and the required risk neutralization activities are undertaken within the framework of the information security control concerned with the geoinformation technologies of an industrial plant. These methods and models allow identification of threats for information assets and their protection sensibilities, evaluation of their implementability, a well as determination of impact they can exert on performance of geoinformation systems at an industrial plant. The risks in information security are neutralized by means of influencing components of these risks, i.e. sensibilities, threats, assets or safety control tools. The research demonstrates the basic effects due to the introduction of the integrated information security system concerned with geoinformation technologies in the sphere of prompt incident response: reduction in package inputs owing to technology replication and due to effect of introduction scale of a geoinformation system, improvement of information security and decrease of risks, as well as mitigation of damage because of cyberattacks.

Key words: risks in information security of geoinformation technologies, evaluation of sensibilities, assessment of threats, information assets value, control tools in information security of geoinformation technologies, risk assessment and management, risk neutralization activities, information protection in geoinformation systems, cyberattack-inflicted damage, prompt incident response.

For citation: Goncharenko S. N., Yakheev V. V. Computer modeling of corporate information security of geoinformation technologies at industrial facilities. *MIAB. Mining Inf. Anal. Bull.* 2022;(2):81-96. [In Russ]. DOI: 10.25018/0236_1493_2022_2_0_81.

Введение

Оценка рисков информационной безопасности (ИБ) геоинформационных технологий (ГИС) промышленного предприятия проводится в следующих случаях: при проведении внутренних аудитов ИБ; при проведении проверок ИБ со стороны руководства промышленного предприятия; при заключении соглашений о сотрудничестве со сторонними организациями; при выборе средств управления безопасностью; при проведении оценки эффективности используемых средств управления безопасностью; в порядке проведения аудитов второй стороны, в том числе дочерних и зависимых организаций; в иных случаях, предусмотренных контрактами или внутренними документами промышленного предприятия; при проведении монито-

ринга инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия [1–3].

Общее описание процесса оценки рисков ИБ приведено на рис. 1 [4, 5].

Методы

Общий процесс оценки активов состоит из идентификации активов и определения их ценности для промышленного предприятия [6].

Определению ценности подлежат активы, имеющие прямое или косвенное влияние на бесперебойную работу геоинформационных систем промышленного предприятия, конфиденциальность [7, 8].

Ценность актива отражает его важность для достижения промышленным предприятием своих целей. Ценность актива рассчитывается в соответствии с классификацией геоинформационных активов. Результатом процесса определения ценности активов является полный перечень защищаемых активов с указанием их ценности.

Значение вероятности реализации угрозы определяется результатами оценки уязвимостей, оценки угроз и определения эффективности средств управления информационной безопасностью ГИС-технологий промышленного предприятия.

Соответственно, значение вероятности реализации угрозы вычисляется по следующей формуле:

$$В_{ру} = К_{уяз} * С_{у} * Ч_{ру} * (100 - Э_{суб})/100$$

$$Э_{суб} = 0\%$$

$$Э_{суб} = 100\%$$

$$Р = Ц_{а} * В_{ру}$$

$$Вес = \sum_{i=1}^{i=9} i * n_i \,, \qquad (1)$$

где $В_{ру}$ — вероятность реализации угрозы; $К_{уяз}$ — критичность уязвимости (от 1 до 3 баллов); $С_{у}$ — сила угрозы (от 1

Рис. 1. Процесс оценки рисков информационной безопасности промышленного предприятия
Fig. 1. Chart of information security risk assessment at a production plant

до 3 баллов); $Ч_{ру}$ — частота реализации угрозы (от 1 до 5 баллов); $Э_{суб}$ — эффективность средств управления безопасностью (от 0 до 100%).

Оценка критичности уязвимостей. Идентификация уязвимостей

Основными источниками информации для идентификации уязвимостей являются: отчеты аудиторов (внутренних и внешних); результаты процесса мониторинга инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия; экспертные мнения (например, риск-менеджеров, менеджеров, консультантов) [9, 10].

Наличие уязвимости означает несоответствие одному или более из применимых требований ИБ.

Критичность уязвимости определяется: ее характером (техническая, нормативная или организационная); степенью несоответствия нарушенному требованию ИБ.

Уязвимость означает недостаток материально-технического, нормативного или организационного обеспечения процессов информационной безопасностью ГИС-технологий промышленного предприятия. Соответственно, тип уязвимости может быть: «техническим», например, нарушение функционала оборудования и/или программного обеспечения, его количества и т.п.; «нормативным», например, некорректность содержания или формы документа, его отсутствие и т.п.; «организационным», например, не назначено ответственное лицо, или не определены требования к компетенциям и т.п.

Степень несоответствия нарушенному требованию информационной безопасности ГИС-технологий промышленного предприятия варьируется следующим образом: «соответствие с замечанием» — требование в целом выполняется, это подтверждается записями и регламентирующими документами. Однако есть незначительные недостатки в документировании и/или в исполнении данного требования; «частичное соответствие» — присутствуют значительные недостатки в документировании и/или исполнении требования; «несоответствие» — присутствуют критичные недостатки в документировании и/или исполнении требования. Например, отсутствие документирования или отсутствие подтверждений исполнения требования.

Для последующего выбора необходимых средств управления информационной безопасностью ГИС-технологий промышленного предприятия определяется причина возникновения данного несоответствия, а также тип этой причины (технический, нормативный или организационный).

Значения критичности уязвимостей определяются целыми цифрами от 1 до 3: значение «1» — «низкая критичность»; значение «2» — «средняя кри-

Таблица 1

Определение критичности уязвимостей
Identification of criticality of sensibilities

		Степень соответствия требованию		
		соответствие с замечанием	**частичное соответствие**	**несоответствие**
Тип уязвимости	техническая	1	1	2
	нормативная	1	2	3
	организационная	2	3	3

тичность»; значение «3» — «высокая критичность.

Значения критичности уязвимостей определяются по табл. 1.

Оценка угроз состоит в определении типа угроз, силы угроз и частоты реализации угроз [11–13].

На основании выявленных уязвимостей определяются способы их реализации (эксплуатации) угрозами ИБ, например, «прекращение электроснабжения оборудования», «кража средства обработки информации», «пожар» и т.д.

ИБ означает обеспечение конфиденциальности, целостности и доступности информации. Соответственно, все угрозы подразделяются на семь основных типов, указанных в табл. 2.

Сила угрозы определяется возможным масштабом ее воздействия, которое может распространяться на:

- отдельные подразделения и/или процессы;
- группы подразделений и/или процессы;
- все промышленное предприятие в целом и/или партнеров (клиентов).

Значения силы угрозы измеряются целыми цифрами от 1 до 3 и определяются согласно табл. 3.

Значение частоты реализации угрозы измеряется целыми цифрами от 1 до 5 и определяется на основании статистических данных, как показано в табл. 4.

Таблица 2

Определение типа угроз информационной безопасности
Identification of information security threats

Тип угрозы	Общие угрозы
Кража	угрозы конфиденциальности
Утечка	
Модификация	угрозы целостности
Подмена	
Утрата доверия	
Блокирование	угрозы доступности
Уничтожение	

Таблица 3

Определение силы угрозы
Determination of strength of threat

	Возможность воздействия на		
	отдельные подразделения и/или процессы	**группы подразделений и/или процессы**	**все промышленное предприятие в целом и/или партнеров / клиентов**
Сила угрозы	1	2	3

Таблица 4

Определение частоты реализации угрозы
Determination of frequency of threat

Частота реализации угрозы		
Значение	**Содержание**	**Частота реализации**
1	никогда не случается	не происходило за последние 3 (три) года
2	редко	раз в год
3	периодически	раз в квартал
4	регулярно	раз в 2 (две) недели
5	часто	раз в неделю

Таблица 5

Оценка эффективности средств управления информационной безопасностью
Efficiency evaluation of information security tools

	Используемый вариант обработки рисков ИБ			
	модификация, %	**распределение, %**	**сохранение, %**	**ликвидация, %**
Исправление, направленное на устранение несоответствия	до 45	до 45	до 50	до 50
Превентивные действия, направленные на устранение причины несоответствия	до 45	до 45	до 50	до 50
Итоговая эффективность средств управления безопасностью ($Э_{суб}$)	(45+45), т.е. до 90	(45+45), т.е. до 90	(50+50), т.е. до 100	(50+50), т.е. до 100

Оценка средств управления информационной безопасностью ГИС-технологий промышленного предприятия. Идентификация используемых средств управления информационной безопасностью геоинформационных систем

Угрозы могут реализоваться только путем эксплуатации существующих уязвимостей, которые означают несоответствие применимым требованиям ИБ. Средства управления безопасностью направлены на нейтрализацию существующих несоответствий, а также предупреждение их появления в будущем.

Средство управления информационной безопасностью геоинформационных систем может быть различной природы: правовой нормой, организационной мерой или техническим средством. При принятии решения о выборе направлений защиты следует учитывать, что наибольший эффект дает применение комплекса мер различной природы и реализации процедур мониторинга инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия [14–17].

Определение эффективности средств управления безопасностью

Значение эффективности средства управления безопасностью является понижающим коэффициентом для критичности уязвимости, измеряется в процентах и определяется экспертным путем:

$Э_{суб}$ = 0% — означает отсутствие влияния средств управления безопасностью на рассматриваемую уязвимость;

$Э_{суб}$ = 100% — означает полную нейтрализацию рассматриваемой уязвимости.

Значение $Э_{суб}$ определяется двумя факторами: применяемые варианты обработки рисков ИБ (стандарт ISO/IEC 27005); полнота устранения самого несоответствия и его причины, т.е. полнота исправления и превентивных действий. Соответственно, значение эффективности средства управления информационной безопасностью геоинформационных систем определяется как сумма эффективности действий по устранению самого несоответствия и его причины.

Возможные варианты расчета значения эффективности средства управления безопасностью представлены в табл. 5.

Результаты

Определение уровней рисков информационной безопасности геоинформационных систем

На основании результатов проведенных выше оценок вычисляется уровень риска ИБ по следующей формуле:

Таблица 6

Основные критерии риска ИБ
Main risk criteria in information security

Наименование критерия риска ИБ	Доля от максимального риска ИБ, %	Соответствующая величина уровня риска ИБ, баллы
Приемлемые риски	13,3	54
Обрабатываемые риски	26,6	108

$$P = Ц_а * В_{ру} \quad (2)$$

где P — уровень риска ИБ (от 0 до 405); $Ц_а$ — ценность актива (от 1 до 9); $В_{ру}$ — вероятность реализации угрозы (от 0 до 45).

Оценивание рисков информационной безопасности геоинформационных систем

Результатом процесса оценивания рисков ИБ является перечень рисков информационной безопасности геоинформационных систем, в котором риски должны быть распределены по степени их важности/опасности. Оценивание риска ИБ заключается в сравнении вычисленного ранее уровня риска ИБ с критериями риска ИБ. Соответственно, в промышленном предприятии должны быть определены критерии риска ИБ [18–20].

Определение критериев риска ИБ

Критерии риска информационной безопасности геоинформационных систем определяются как процентная доля от максимального риска ИБ. Реализация максимального риска ИБ означает нанесение ущерба (превышающего риск-аппетит, определение которого регламентировано внутренними документами по управлению рисками) промышленному предприятию, который может привести к ликвидации промышленного предприятия. Возможность нанесения такого ущерба соответствует уровню риска информационной безопасности геоинформационных систем в 405 баллов [21–23]. В соответствии с этим выделены следующие основные критерии риска ИБ, как показано в табл. 6.

Также выделены следующие дополнительные критерии риска ИБ, как показано в табл. 7.

Категорирование рисков информационной безопасности

Категорирование рисков информационной безопасности геоинформационных систем заключается в разделении

Таблица 7

Дополнительные критерии риска
Additional risk criteria

Наименование критерия риска ИБ	Доля от максимального риска ИБ, %	Соответствующая величина уровня риска ИБ, баллы
Нерассматриваемые риски ИБ	3,5	14
Незначительные риски ИБ	6,7	27
Средние риски ИБ	41,5	168
Существенные риски ИБ	55,5	225
Высокие риски ИБ	70,4	285
Очень высокие риски ИБ	80	324

Таблица 8

Подкатегории рисков ИБ
Subcategories of risks in information security

Категория риска ИБ	Подкатегории риска ИБ	Нижний предел риска ИБ, баллы	Верхний предел риска ИБ, баллы
	наименование		
Приемлемые	нерассматриваемый	0	14
	незначительный	15	27
	очень низкий	28	54
Обрабатываемые	низкий	55	108
Критичные	средний	109	168
	существенный	169	225
	высокий	226	285
	очень высокий	286	324
	разрушительный	325	405

рисков ИБ в зависимости от степени их опасности на отдельные категории.

Категорирование рисков информационной безопасности геоинформационных систем выполняется по результатам сравнения уровней рисков ИБ с критериями риска ИБ. Соответственно, выделены следующие основные категории рисков ИБ: «Приемлемые» — (величиной от 0 до 54 баллов включительно), в отношении которых не предпринимаются никаких активных действий по нейтрализации. Данные риски информационной безопасности геоинформационных систем подлежат мониторингу с целью своевременного выявления негативных тенденций их роста; «Обрабатываемые» — (свыше 54 до 108 баллов включительно), которые подлежат обработке в плановом порядке; «Критичные» — (свыше 108 до 405 включительно), подлежащие обработке в приоритетном порядке.

В свою очередь, основные категории рисков ИБ в соответствии с дополнительными критериями риска ИБ разделяются на подкатегории так, как показано в табл. 8. Категорирование необходимо для получения баллов верхних и нижних пределов риска информационной безопасности геоинформационных систем.

Обработка рисков информационной безопасности

Определение «веса» уязвимостей. Для последующей обработки рисков ИБ необходимо определить наиболее критичные уязвимости. Для этого определяется «вес» уязвимости.

Нейтрализация обрабатываемых и критичных рисков ИБ производится в соответствии с планом мониторинга инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия. При формировании плана обработки рисков информационной безопасности геоинформационных систем необходимо определить последовательность реализации мер по их обработке, т.е. последовательность внедрения необходимых средств управления безопасностью. С другой стороны, средства управления безопасности направлены на устранение выявленных несоответствий и нейтрализацию связанных с этими несоответствиями уязвимостей. При этом одна и та же уязвимость может вызывать ряд рисков ИБ различной величины, направленных на

различные активы. Последовательность обработки выявленных рисков информационной безопасности геоинформационных систем определяется степенью опасности существующих уязвимостей СУИБ, и обработка начинается с нейтрализации наиболее опасных уязвимостей. С целью определения относительной опасности уязвимостей используется такая вспомогательная величина, как «вес» уязвимости. Вес уязвимости учитывает количество и уровни рисков ИБ, обусловленных наличием данной уязвимости.

Вес уязвимости вычисляется по следующей формуле:

$$Вес = \sum_{i=1}^{i=9} i * n_i \,, \qquad (3)$$

где *Вес* — вес уязвимости; i — номер подкатегории рисков ИБ; n_i — количество обусловленных данной уязвимостью рисков ИБ i-й подкатегории.

Последовательность обработки риска ИБ

После определения соответствующих рисков ИБ, которые подлежат дальнейшему анализу, выполняются последовательно следующие действия: сортировка по «весу» уязвимости; выбор стратегии обработки риска ИБ (сокращение, перераспределение, принятие или уклонение); идентификация необходимых средств управления безопасностью и оценка их эффективности); заново рассчитываются уровни рисков ИБ; проводится оценка рисков ИБ, результат оценивается по критериям риска ИБ.

Критерии эффективности использования оценки рисков ИБ

Критериями результативности оценки рисков ИБ промышленного предприятия являются: своевременность утверждения планов обработки рисков ИБ; учет результатов оценки рисков ИБ при принятии важных управленческих решений; статистика событий и инцидентов ИБ, а также величина вызванного ими ущерба.

Мониторинг и управление процессом оценки рисков информационной безопасности геоинформационных систем

Мониторинг своевременности и полноты проведения оценки рисков ИБ осуществляется службой безопасности (СБ).

СБ предоставляет руководству промышленного предприятия результаты оценки рисков ИБ с описанием проведенных мероприятий, используемых систем защиты и текущих угроз. Ключевой рисковый показатель используется для мониторинга ключевых рисков ИБ.

Таблица 9

Расчеты ценности актива
Valuation of assets

Этап 1. Идентификация актива	**Этап 2. Определение требований к конфиденциальности**	**Этап 3. Определение требований к целостности**	**Этап 4. Определение требований к доступности**	**Этап 5. Определение ценности актива**
актив	**конфиденциальность (К)**	**целостность (Ц)**	**доступность (Д)**	**ценность информационного актива**
Данные о заработной плате работников Промышленного предприятия	3	3	2	3 +3 + 2 = 8

Таблица 10

Расчет уровня риска информационной безопасности
Calculation of risk level in information security

Действие	Объект действия	Результат действия	
		величина	значение
определение ценности актива	актив — данные о заработной плате работников промышленного предприятия	ценность актива (3+3+2)	8
определение критичности уязвимости	уязвимость — отсутствие утвержденной процедуры предоставления доступа к информационным системам	высокая критичность (уязвимость нормативная + несоответствие стандарту = 3)	3
определение силы угрозы	угроза — утечка или ошибки в данных	высокая сила угрозы (на все промышленное предприятие = 3)	3
определение частоты реализации угрозы	частота появления ошибок	редко (раз в год = 2)	2
определение эффективности защиты	средства управления безопасностью	отсутствие влияния на рассматриваемую уязвимость	0%
определение вероятности реализации угрозы	появление ошибок	вероятность реализации угрозы (3*3*2=18)	18
вычисление уровня риска ИБ	вышеопределенные величины: строки 1 и 6	уровень риска ИБ (8*18)	144

Мониторинг инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия осуществляется раз в два года или чаще, по мере необходимости.

Сроки и периодичность предоставления результатов оценки рисков ИБ руководству промышленного предприятия определяются в соответствии со сроками и периодичностью регламентированных в правилах внутреннего аудита ИБ.

Ответственность и контроль

Ответственность за организацию и контроль процесса оценки рисков информационной безопасности геоинформационных систем в промышленном предприятии несет начальник СБ.

Ответственность за процесс нейтрализации рисков ИБ несут владельцы активов, за организацию данного процесса — начальник СБ.

Ответственность за идентификацию и оценку новых рисков ИБ несет менеджер СБ, на основе сведений об изменениях в информационных активах и информационной системе промышленного предприятия, предоставляемых владельцами данных активов.

Ответственность за доведение информации о текущих рисках ИБ до высшего руководства промышленного предприятия несет начальник СБ.

Пример опросника для заполнения реестра активов (табл. 9, 10).

Обсуждение результатов

Рекомендации по формированию плана обработки рисков информационной безопасности

План обработки рисков информационной безопасности геоинформационных систем представляют собой перечень необходимых к внедрению мер безопас-

Рис. 2. Комплекс решений компании по обеспечению информационной безопасности
Fig. 2. Package of corporate decisions on information security

ности с указанием сроков их реализации и исполнителей. План обработки рисков ИБ предназначен для представления высшему руководству с целью рассмотрения и утверждения намеченных мер защиты. План обработки рисков ИБ составляется на основании плана нейтрализации уязвимостей, в котором определена последовательность нейтрализации выявленных уязвимостей. План обработки уязвимостей предназначен для специалистов, выполняющих реализацию намеченных мер защиты. Последовательность реализации необходимых мер безопасности, в свою очередь, определяется относительной опасностью выявленных уязвимостей, т.е. их «весом». При первичной обработке рисков ИБ нейтрализация критичных рисков ИБ заключается в переводе их в группы обрабатываемых и/или приемлемых, а обрабатываемых — в группу приемлемых. При оценке рисков ИБ выполняется оценка регламентированности и исполнения применимых мер управления ИБ. В целях дальнейшей нейтрализации обрабатываемых рисков ИБ рекомендуется по завершении внедрения выбранных средств защиты применить общее средство — проведение внеочередного аудита ИБ с оценкой рисков ИБ. По результатам данной оценки рисков ИБ принимается решение о необходимости дальнейшей обработки рисков ИБ и составления соответствующего плана обработки рисков ИБ.

Рис. 3. Анализ корпоративных рисков и угроз в сфере ИБ
Fig. 3. Analysis of corporate risks and threats in the sphere of information security

Рис. 4. Структура корпоративной комплексной системы информационной безопасности КСИБ
Fig. 4. Structure of corporate integrated information security system

Внедрение комплексной системы информационной безопасности геоинформационных систем промышленного предприятия

Целью внедрения комплексной системы информационной безопасности является обеспечение надежной, гибкой и современной системой информационной безопасности (рис. 2).

Анализ рисков и числа угроз промышленного предприятия по состоянию позволил выявить следующую статистику (рис. 3). Сумма простоя информационных систем компании при взломе составила 938,4 млрд у.е. при средней стоимости утечки информации 85 млрд у.е.

Анализ полученных величин ущерба являлся базисной предпосылкой созда-

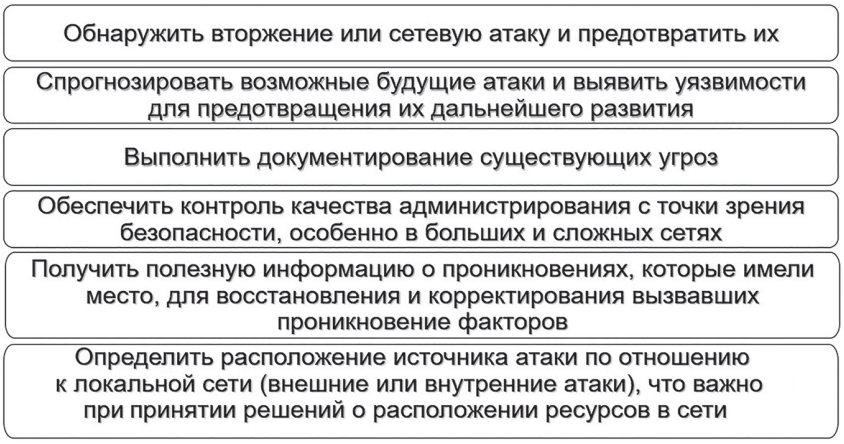

Рис. 5. Основные функции корпоративной системы информационной безопасности
Fig. 5. Main functions of corporate information security system

Рис. 6. Основные эффекты внедрения корпоративной системы информационной безопасности
Fig. 6. Main introduction effects of corporate information security system

ния корпоративной системы информационной безопасности ГИС-технологий промышленного предприятия (рис. 4).

Основные функции корпоративной комплексной системы информационной безопасности (КСИБ) заключаются в следующем (рис. 5).

Заключение

Таким образом, исходя из проведенных исследований, основные эффекты от внедрения корпоративной системы информационной безопасности ГИС-технологий промышленного предприятия будут получены в сфере оперативного реагирования на инциденты, снижения комплексных затрат за счет тиражирования технологии и эффекта масштаба внедрения ИТ, повышения уровня ИБ и снижения факторов риска, а также за счет снижения ущерба от постоянных кибератак (рис. 6).

При этом основная цель процесса управления информационной безопасностью заключающаяся в минимизации рисков негативного воздействия на стабильность и целостность промышленной среды предприятия, достигнута и реализуется в рамках процесса осуществления плана мероприятий по отработке рисков информационной безопасности и принятия решений в соответствии с существующими практиками и правилами внедрения релизов в сфере ГИС-технологий промышленного предприятия. Кроме того, происходит обеспечение баланса между текущими и будущими потребностями промышленного предприятия в доступности и мощности ИТ-услуг, а также эффективности затрат на предоставление ИТ-услуг.

Данный процесс обеспечивает осуществление оценки текущих возможностей, реализацию процедуры мониторинга инцидентов геоинформационной системы безопасности управления деятельностью промышленного предприятия, прогнозирование будущих потребностей, а также на основе оценки рисков информационной безопасности выявление и уточнение требований промышленного предприятия к ИТ-услугам, ГИС-технологиям и системам, проектирование, согласование и последующий мониторинг качества и доступности ГИС.

СПИСОК ЛИТЕРАТУРЫ

1. *Салахутдинова К. И.*, *Лебедев И. С.*, *Кривцова И. Е.* Подход к выбору информативного признака в задаче идентификации программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики. — 2018. — Т. 18. — № 2. — С. 278—285.

2. *Alladi T., Chamola V., Parizi R. M., Kim-Kwang Raymond Choo* Blockchain applications for Industry 4.0 and Industrial IoT: A review // IEEE Access. 2019, vol. 7, pp. 176935—176951.

3. *Запечников С. В.*, *Милославская Н. Г.* Информационная безопасность открытых систем. В 2-х т. Т. 1 — Угрозы, уязвимости, атаки и подходы к защите. — М.: ГЛТ, 2017. — 536 с.

4. *Запечников С. В.*, *Милославская Н. Г.*, *Толстой А. И.*, *Ушаков Д. В.* Информационная безопасность открытых систем. В 2-х т. Т. 2 — Средства защиты в сетях. — М.: ГЛТ, 2018. — 558 с.

5. *Минаев В. А.*, *Сычев М. П.*, *Вайц Е. В.*, *Грачева Ю. В.* Моделирование угроз информационной безопасности с использованием принципов системной динамики // Вопросы радиоэлектроники. — 2017. — № 6. — С. 75—82.

6. *Минаев В. А.*, *Сычев М. П.*, *Вайц Е. В.*, *Грачева Ю. В.* Риск-ориентированный подход к моделированию процесса противодействия угрозам информационной безопасности // Вопросы радиоэлектроники. — 2017. — № 6. — С. 83—92.

7. *Casinoa F.*, *Dasaklis T. K.*, *Patsakis C. A.* Systematic literature review of blockchain-based applications: Current status, classification and open issues // Telematics and Informatics. 2019, vol. 36, pp. 55—81.

8. *Marques M.* Decentralized decision support for intelligent manufacturing in Industry 4.0 // Journal of Ambient Intelligence and Smart Environments. 2017, vol. 9, no 3, pp. 299—313.

9. *Чипига А. Ф.* Информационная безопасность автоматизированных систем. — М.: Гелиос АРВ, 2017. — 336 с.

10. *Коробец Б. Н.*, *Минаев В. А.*, *Сычев М. П.* Информационные операции и проблема формирования современной культуры информационной безопасности // Системы высокой доступности. — 2017. — Т. 13. — № 3. — С. 38—46.

11. *Temkin I. O., Myaskov A. V., Deryabin S. A., Rzazade U. A.* Digital twins and modeling of the transporting-technological processes for on-line dispatch control in open pit mining // Eurasian Mining. 2020, vol. 2, pp. 55–58.

12. *Ramakrishna S.*, *Khong T. H.*, *Leong T. K.* Smart manufacturing // Procedia Manufacturing. 2017, vol. 12, pp. 128—131.

13. *Xifan Yao, Jiajun Zhou, Yingzi Lin, Yun Li, Hongnian Yu, Ying Liu* Smart manufacturing based on cyber-physical systems and beyond // Journal of Intelligent Manufacturing. 2019, vol. 30, no. 1, pp. 2805—2817.

14. *Умербеков Ж. Ж.*, *Гончаренко С. Н.* Обоснование эффективности внедрения целевой модели управления производственной безопасностью горнодобывающей компании // Горный информационно-аналитический бюллетень. — 2019. — № 8. — С. 225–234. DOI: 10.25018/0236-1493-2019-08-0-225-234.

15. *Быкова В. В.*, *Катаева А. В.* Методы и средства анализа информативности признаков при обработке медицинских данных // Программные продукты и системы. — 2016. — № 2. — С. 172—178.

16. *Vacca J. R.* Computer and Information Security Handbook. Elsevier, 2017, 1280 p.

17. *Vostrikov A. V.*, *Prokofeva E. N.*, *Goncharenko S. N.*, *Gribanov I. V.* Analytical modeling for the modern mining industry // Eurasian Mining. 2019, no. 2, pp. 30—35. DOI: 10.17580/em.2019.02.07.

18. *Ералин Ж. М.*, *Гончаренко С. Н.* Разработка моделей решения ключевых проблем стратегического развития уранодобывающего предприятия // Горный информационно-аналитический бюллетень. — 2019. — № 4. — С. 199–208. DOI: 10.25018/0236-1493-2019-04-0-199-208.

19. *Милославская Н. Г.*, *Толстой А. И.* Визуализация процессов управления информационной безопасностью // Научная визуализация. — 2017. — Т. 9. — № 5. — С. 117—136.

20. *Ревенков П. В.*, *Бердюгин А. А.* Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. — 2017. — № 3(21). — С. 16—23.

21. *Trofimov V. B.* Prototype approach to design of the automated expert systems with multistructural recognition of complex images // Automation and Remote Control. 2016, vol. 77, no. 6, pp. 1115–1121.

22. *Пешкова М. Х.*, *Попов С. М.*, *Стоянова И. А.* Методические основы оценки емкости локальных рынков при организации производства продукции из горнопромышленных отходов // Горный журнал. — 2017. — № 4. — С. 39—43.

23. *Гончарова А. Р.*, *Стоянова И. А.* Характеристика геоэкологических локальных условий строительства коммуникаций для обеспечения транзита продукции добывающих отраслей // Горный информационно-аналитический бюллетень. — 2020. — № 6-1. — С. 163—175. DOI: 10.25018/0236-14932020-61-0-163-175. ГИАБ

REFERENCES

1. Salakhutdinova K. I., Lebedev I. S., Krivtsova I. E. An approach to the selection of an informative feature in the problem of software identification. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki*. 2018, vol. 18, no. 2, pp. 278—285. [In Russ].

2. Alladi T., Chamola V., Parizi R. M., Kim-Kwang Raymond Choo Blockchain applications for Industry 4.0 and Industrial IoT: A review. *IEEE Access*. 2019, vol. 7, pp. 176935—176951.

3. Zapechnikov S. V., Miloslavskaya N. G. *Informatsionnaya bezopasnost' otkrytykh sistem. T. 1. Ugrozy, uyazvimosti, ataki i podkhody k zashchite* [Information security of open systems. Vol. 1 Threats, vulnerabilities, attacks and approaches to defense], Moscow, GLT, 2017, 536 p.

4. Zapechnikov S. V., Miloslavskaya N. G. *Informatsionnaya bezopasnost' otkrytykh sistem. T. 2. Sredstva zashchity v setyakh* [Information security of open systems. Vol. 2 Means of protection in networks], Moscow, GLT, 2018, 558 p.

5. Minaev V. A., Sychev M. P., Vayts E. V., Gracheva Yu. V. Modeling information security threats using the principles of system dynamics. *Issues of radio electronics*. 2017, no. 6, pp. 75—82. [In Russ].

6. Minaev V. A., Sychev M. P., Vayts E. V., Gracheva Yu. V. Risk-based approach to modeling the process of countering information security threats. *Issues of radio electronics*. 2017, no. 6, pp. 83—92. [In Russ].

7. Casinoa F., Dasaklis T. K., Patsakis C. A. Systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*. 2019, vol. 36, pp. 55—81.

8. Marques M. Decentralized decision support for intelligent manufacturing in Industry 4.0. *Journal of Ambient Intelligence and Smart Environments*. 2017, vol. 9, no 3, pp. 299—313.

9. Chipiga A. F. *Informatsionnaya bezopasnost' avtomatizirovannykh sistem* [Information security of automated systems], Moscow, Gelios ARV, 2017, 336 p.

10. Korobets B. N., Minaev V. A., Sychev M. P. Information operations and the problem of forming a modern information security culture. *Sistemy vysokoy dostupnosti*. 2017, vol. 13, no. 3, pp. 38—46. [In Russ].

11. Temkin I. O., Myaskov A. V., Deryabin S. A., Rzazade U. A. Digital twins and modeling of the transporting-technological processes for on-line dispatch control in open pit mining. *Eurasian Mining*. 2020, vol. 2, pp. 55–58.

12. Ramakrishna S., Khong T. H., Leong T. K. Smart manufacturing. *Procedia Manufacturing*. 2017, vol. 12, pp. 128—131.

13. Xifan Yao, Jiajun Zhou, Yingzi Lin, Yun Li, Hongnian Yu, Ying Liu Smart manufacturing based on cyber-physical systems and beyond. *Journal of Intelligent Manufacturing*. 2019, vol. 30, no. 1, pp. 2805—2817.

14. Umerbekov Zh. Zh., Goncharenko S. N. Validation of efficiency of the target production safety management model introduction in the mining industry. *MIAB. Mining Inf. Anal. Bull.* 2019, no. 8, pp. 225–234. [In Russ]. DOI: 10.25018/0236-1493-2019-08-0-225-234.

15. Bykova V. V., Kataeva A. V. Methods and tools for analyzing the informativeness of signs in the processing of medical data. *Programmnye produkty i sistemy*. 2016, no. 2, pp. 172—178. [In Russ].

16. Vacca J. R. *Computer and Information Security Handbook*. Elsevier, 2017, 1280 p.

17. Vostrikov A. V., Prokofeva E. N., Goncharenko S. N., Gribanov I. V. Analytical modeling for the modern mining industry. *Eurasian Mining*. 2019, no. 2, pp. 30—35. DOI: 10.17580/em.2019.02.07.

18. Yeralin Z. M., Goncharenko S. N. Models for solving key problems of strategic development of uranium mines. *MIAB. Mining Inf. Anal. Bull.* 2019, no. 4, pp. 199–208. [In Russ]. DOI: 10.25018/0236-1493-2019-04-0-199-208.

19. Miloslavskaya N. G., Tolstoy A. I. Visualization of information security management processes. *Nauchnaya vizualizatsiya*. 2017, vol. 9, no. 5, pp. 117—136. [In Russ].

20. Revenkov P. V., Berdyugin A. A. Expansion of the operational risk profile in banks with an increase in DDoS threats. *Voprosy kiberbezopasnosti*. 2017, no. 3(21), pp. 16—23. [In Russ].

21. Trofimov V. B. Prototype approach to design of the automated expert systems with multistructural recognition of complex images. *Automation and Remote Control*. 2016, vol. 77, no. 6, pp. 1115–1121.

22. Peshkova M. KH., Popov S. M., Stoyanova I. A. Methodical basis for assessment of local market capacity for manufacture of products from mining waste. *Gornyi Zhurnal*. 2017, no. 4, pp. 39—43. [In Russ].

23. Goncharova A. R., Stoyanova I. A. Characteristics of geoecological local conditions for the construction of communications to ensure the transit of products from extractive industries. *MIAB. Mining Inf. Anal. Bull.* 2020, no. 6-1, pp. 163—175. [In Russ]. DOI: 10.25018/0236-14932020-61-0-163-175.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гончаренко Сергей Николаевич — д-р техн. наук,
профессор, НИТУ «МИСиС», e-mail: gsn@misis.ru,
http://orcid.org/0000-0001-7783-3738,
Яхеев Валерий Васильевич — канд. техн. наук, доцент,
Санкт-Петербургский университет
Государственной противопожарной службы МЧС России,
e-mail: yakvaleri@yandex.ru.
Для контактов: Гончаренко С.Н., e-mail: gsn@misis.ru.

INFORMATION ABOUT THE AUTHORS

S.N. Goncharenko, Dr. Sci. (Eng.), Professor,
National University of Science and Technology «MISiS»,
119049, Moscow, Russia, e-mail: gsn@misis.ru,
http://orcid.org/0000-0001-7783-3738.
V.V. Yakheev, Cand. Sci. (Eng.), Assistant Professor,
Saint-Petersburg University of State Fire Service of Emercom of Russia,
190000, Saint Petersburg, Russia, e-mail: yakvaleri@yandex.ru.
Corresponding author: S.N. Goncharenko, e-mail: gsn@misis.ru.

Получена редакцией 24.11.2021; получена после рецензии 10.12.2021; принята к печати 10.01.2022.
Received by the editors 24.11.2021; received after the review 10.12.2021; accepted for printing 10.01.2022.