В случае возбуждения уголовного дела знаменитому вратарю грозило бы до восьми лет лишения свободы. Прокуратура города Пардубице, в котором проходил матч, после рассмотрения обстоятельств инцидента приняла решение не возбуждать уголовное дело. В марте нынешнего года (2004. — А.С.) это решение было подтверждено, после чего апелляцию с требованием привлечь Гашека к ответственности подал пострадавший Мартин Шила. Районный прокурор Пардубице Ленка Стрнадова приняла окончательное решение не возбуждать дела против Гашека. «Нападение действительно имело место, но оно не было столь жестоким, чтобы нанести серьезный вред здоровью пострадавшего», — обосновала она свое решение в интервью газете «Блеск». Легендарному вратарю теперь грозит лишь административное взыскание: штраф в размере 3 тысяч крон (около $120)».

В уголовных кодексах ряда стран (Китайской народной республики, республики Болгарии, Голландии) вопросы, связанные с квалификацией причинения вреда жизни или здоровью при занятиях спортом, не нашли отражения.

В заключение можно сделать вывод, что уголовное законодательство большинства названных зарубежных стран не признает преступлением причинение вреда жизни или здоровью при занятиях спортом, рассматривая его в качестве обстоятельства, исключающего преступность деяния или уголовную ответственность и наказуемость при условии, что соответствующий вид деятельности разрешен законом и установленные для него правила не должны быть нарушены.

Список литературы

1. Грызыхин С.А. Отягчающие обстоятельства убийства по зарубежному уголовному законодательству // Вестник Омского университета. Серия: Право. 2008. № 2. С.145-150.

2. Оганесян Л.Р. Возраст уголовной ответственности в уголовном праве зарубежных стран (США, Англия, Франция, Австрия, Швейцария, Испания, ФРГ, Япония // Вектор науки Тольяттинского государственного университета. 2009. № 2 (5). С.113-115.

3. Уголовное право зарубежных государств. Общая часть: Учебное пособие / под ред. И.Д. Козочкина. - М.: Омега-Л. 2003. - 576 с.

4. Козочкин И.Д. Уголовное право зарубежных государств. Общая часть: Учебное пособие / Под ред. и с предисл. И.Д. Козочкина. — М.: Омега-Л, Институт международного права и экономики им. А.С. Грибоедова,2003. - 576 с.. 2003.

ТРЕБОВАНИЯ ПО СОЗДАНИЮ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АСУ ТП НА ОСНОВЕ ЗАРУБЕЖНЫХ СТАНДАРТОВ

Александрова Алина Викторовна
Студентка 4 курса факультета Информационных технологий
Московского политехнического университета

Широков Анатолий Александрович
Студент 4 курса факультета Информационных технологий
Московского политехнического университета

Еникеев Ильдар Хасанович
доктор технических наук, профессор, профессор кафедры
«Математика» Московского политехнического университета

Аннотация: *В данной статье проведено сравнение требования российских и зарубежных регуляторов по защите информации, к которым в той или иной степени могут быть применимы системы защиты от утечек.*

Ключевые слова: *требования безопасности, безопасность АСУ ТП, процесс управления.*

Abstract: *This article compares the requirements of Russian and foreign regulators for the protection of information, which in varying degrees may be ap-plicable to the system of protection against leaks.*

Keywords: *security requirements, security of industrial control, process control.*

Ведение. Вопросы обеспечения безопасности автоматизированных си-стем управления технологическим процессами (АСУ ТП) становятся всё акту-альнее. Если несколько лет назад эта тема в основном поднималась среди уз-кого круга специалистов, то сейчас она стала интересна собственникам систем управления, специалистам, занимающимся их эксплуатацией, разработкой и внедрением и законодателям [1, 2].

Проведя сравнение требования российских и зарубежных регуляторов по защите информации, к которым в той или иной степени могут быть при-менимы системы защиты от утечек.Был создан порядок действий по созданию обеспечения безопасности АСУ ТП, далее было проверено наличие этих пунктов в таких документах, как:

- Приказ ФСТЭК России от 25 декабря 2017 г. N 239 (Далее ФСТЭК N239)
- ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникаци-онные промышленные. Защищенность (кибербезопасность) сети и системы (Далее ГОСТ 56205)
- GOOD PRACTICE GUIDE 1-7. PROCESS CONTROL AND SCADA SECURITY (Далее CPNI)
- NIST Special Publication 800-82 Revision 2 (Далее NIST 800-82)

Далее пронумерованы последовательные шаги по выполнению требований, основанных на 4 документах:

№ Шага	Требования		Пункт документа			
			ФСТЭК N239	ГОСТ 56205	CPNI	NIST 800-82
Разработка мер безопасности						
	Разработать процесс управления рисками		-	-	-	3.1.
	Определить важность риска для ICS		-	5.12.2.	-	-
	Установить границу охвата анализа рисков		-	-	1-3.4.1.	-
	Определить критерии допустимости риска для организации		-	5.12.2.	-	-
	Выявить источники угроз и оценить возможности нарушителей		11.1.	5.7.2.	-	-
	Проанализировать возможные уязвимости		11.1.	-	-	-
	Выполнить оценку риска		11.1.	5.7.2.	1-3.4.3.	-
	Определить возможные сценарии реализации угроз ИБ		11.1.	-	1-3.3.	-
	Оценить последствия от реализации угроз ИБ		11.1.	5.7.2.	1-3.3.	-
	Определить степень защиты безопасности для каждого элемента		-	5.12.2.	-	-
	Провести семинар по снижению рисков с целью выбора архитектуры защиты		-	-	2-3.4.2.	-
	Решить, какие действия необходимо осуществить по каждому из рисков		-	-	2-3.4.3.	-

№ Шага	Требования		Пункт документа			
			ФСТЭК N239	ГОСТ 56205	CPNI	NIST 800-82
	Определить план реализации мер безопасности		13.1.	-	2-3.4.4.	-
	Разработать ICS, которая будет соответствовать уровню безопасности		-	5.12.2.	-	-
	Установить контрольный список мер по снижению рисков относительно уровня безопасности		-	5.12.2.	2-3.4.5.	-
	Разработать архитектуру безопасности		-	5.12.2.	-	-
	Разбить задачи по обеспечению безопасности		-	5.7.2.	-	-
	Разделить сеть ICS от корпоративной		-	-	-	5.1.
1.	Сегментировать зоны безопасности		-	6.5.2.	-	-
	Определить ФТБ к зонам предприятия		-	5.7.2.	-	-
	Документировать объекты и субъекты доступа		11.2.	5.7.2	-	5.4
	Минимизировать точек доступа к ICS		-	-	-	5.4
	Выбрать политики управления доступом (дискреционная, мандатная, ролевая, комбинированная)		11.2.	-	-	-
	Согласовать план реализации архитектуры безопасности		-	-	2-3.4.6.	-
	Учесть в обеспечении безопасности возможные последствия, относящиеся к мерам безопасности, действующим в условиях эксплуатации		-	5.12.2.	-	-
	Выбрать и установить многоуровневую разнообразную защиту архитектуры от известных атак		-	-	-	5.6.
	Спроектировать границы и портал управления доступом для защищенных зон и обеспечить их защищенность		-	5.7.2.	-	5.2.
	Определить и обосновать организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта		11.2.	5.7.2.	-	-
	Проанализировать протоколы с точки зрения функции, риска безопасности и предлагаемых мер		-	-	-	5.8.
	Определить виды и типы СЗИ которые будем использовать		11.2.	5.7.2.	-	-

№ Шага	Требования		Пункт документа			
			ФСТЭК N239	ГОСТ 56205	CPNI	NIST 800-82
	Выбрать элементы управления безопасности и их разработка (при необходимости)			5.7.2.	-	4.5.2.
	Разработать архитектуру подсистемы безопасности		11.2.	5.7.2.	-	
	Определить меры безопасности при взаимодействии значимого объекта с иными объектами		11.2.	-	-	-
	Разработать рабочую документацию на значимый объект		11.3.	-	-	-
Внедрение мер безопасности						
	Начать реализацию мер по повышению безопасности		-	-	2-3.4.7.	-
	Установить и настроить средства ЗИ		12.1.	-	-	4.5.4.
	Организовать контроль физического доступа		12.3.	-	-	-
	Реализовать правила разграничения логического доступа		12.3	-	-	-
	Перепроверить организационно-распорядительные документы на полноту информации для персонала		12.3.	-	-	-
	Осуществить предварительное испытание значимого объекта и его подсистем безопасности		12.4.	-	-	-
	Осуществить опытную эксплуатацию значимого объекта		12.5.	-	-	-
	Проанализировать рабочую документацию и организационно-распорядительные документы на потенциальные уязвимости		12.6.	5.7.2.	-	-
	Провести анализ настроек программных и программно-аппаратных средств на уязвимости		12.6.	-	-	-
	Осуществить выявление известных уязвимостей программных и программно-аппаратных средств		12.6.	-	-	-
	Провести тестирование на проникновение в условиях, соответствующих возможностям нарушителей		12.6.	-	-	-
	Осуществить приемочные испытания значимого объекта и его подсистемы безопасности		12.7.	-	-	-

Исходя из результатов проведенного исследования, мы пришли к выводу, что российские стандарты далеко не идеальны, они имеют пробелы и недочеты, особенно при рассмотрении рисков информационной безопасности.

Зарубежные же стандарты допускают использование более усиленных механизмов и требований по защите информации, но несмотря на всю «продвинутость», в документах так же есть пробелы, которые, например, описаны в российских стандартах.

Список литературы

1. Калашниов В.Н. И все же - автоматизированные системы управления.//Эко. - 2001 г. - №12. -,с.68
2. Норенков И.П. Основы автоматизированного проектирования. М.: 2000.-МГТУ им. Баумана.

СПОРНОСТЬ ПРАВОЙ ПРИРОДЫ СЕКРЕТОВ ПРОИЗВОДСТВА (НОУ-ХАУ)

Долгов Сергей Геннадьевич
к.ю.н., доцент, доцент кафедры предпринимательского, трудового и корпоративного права ИПиНБ РАНХиГС при Президенте РФ

Виноградова Дарья Алексеевна
магистр кафедры предпринимательского, трудового и корпоративного права ИПиНБ РАНХиГС при Президенте РФ

Аннотация: *В рамках данной статьи рассматриваются и выявляются основные проблемы касающиеся правовой природы секретов производства (ноу-хау), проводится лексикографическое исследование значений слов и выражений, определяющих терминологию изучаемого объекта, проводится сравнительное исследование изучаемого объекта с характеристиками смежных результатов интеллектуальной деятельности и выделяются его квалифицирующие признаки. Исследуются особенности и правовая природа объектов «ноу-хау». Вскрывается отсутствие единой точки зрения и наличие диаметрально противоположных суждений как в отношении содержания исследуемого объекта интеллектуальных прав, его характеристик, так и в вопросе отсутствия исключительных прав на секреты производства (ноу-хау).*

Ключевые слова: *Ноу-хау, секреты производства, интеллектуальная деятельность, интеллектуальные права, правовая охрана, коммерческая тайна.*

Abstract: *This article examines and identifies the main problems concerning the legal nature of production secrets (know-how), conducts a lexicographic study of the meanings of words and expressions defining the terminology of the object under study, conducts a comparative study of the object under study with characteristics of related results of intellectual activity and identifies its qualifying features. The features and the legal nature of the objects of «know-how.» The author reveals the absence of a common point of view and the presence of diametrically opposed judgments both in relation to the content of the object of intellectual property rights, its characteristics, and in the absence of exclusive rights to the secrets of production (know-how).*

Keywords: *know-how, secrets of production, intellectual activity, intellectual rights, legal protection, trade secret.*

В наше время, время бурного развития рынка научно-технической продукции, в основе научно-технических процессов, всегда лежат новые знания, которые являются результатом интеллектуальной деятельности человека и нуждаются во внимательном отношении к вопросам защиты исключительных, неимущественных прав. Вопрос о ноу-хау (секретах производства) возникает в случаях появления исключительно важных для производственно-хозяйственной деятельности предприятий результатов интеллектуальной деятельности. Секреты производства среди всех иных результатов интеллектуальной деятельности является одним из самых незащищенных и требует тщательного анализа его правовой природы.