DOI: 10.17747/2618-947X-2024-4-360-367
УДК: 004.01
JEL: M15

Комплаенс-риски эксплуатации ИТ-продуктов

В.С. Николаенко[1, 2, 3]
[1] Томский государственный университет систем управления и радиоэлектроники (Томск, Россия)
[2] Томский политехнический университет (Томск, Россия)
[3] Сибирский государственный медицинский университет (Томск, Россия)

Аннотация
В статье рассматриваются комплаенс-риски, которые могут материализоваться во время эксплуатации ИТ-продуктов на рынке и причинить неприемлемый для ИТ-субъектов ущерб. Для достижения поставленной цели автором настоящей статьи было проведено исследование гражданско-правовой, административной и уголовной судебной практики, где одной из сторон являлся ИТ-субъект (ОКВЭД 62), в том числе изучались споры, связанные с нарушением исключительных прав на ИТ-продукты. На основании проведенного исследования было идентифицировано 12 комплаенс-рисков, а именно 6 гражданско-правовых, 1 административный и 5 уголовных. Анализ судебной практики показал, что вывод, распространение и эксплуатация ИТ-продуктов на рынке без учета этих требований грозит для ИТ-субъектов наступлением гражданско-правовой, административной и/или уголовной ответственности. Кроме того, в рамках выполняемой работы была проанализирована динамика совершения уголовных преступлений в сфере компьютерной информации и обнаружено, что в период 2022–2023 годов рост преступлений, связанных с неправомерным доступом к электронным устройствам, увеличился с 9308 до 36 788 случаев (рост составил 74,6%). Полученные результаты в ходе проведенного исследования выявили острую необходимость создания ИТ-субъектами результативных и эффективных превентивных мер воздействия на идентифицированные комплаенс-риски: например, разработку мер, связанных с верификацией требований документального сопровождения ИТ-проектов, формой и содержанием ИТ-продуктов, а также способами защиты компьютерной информации.
Ключевые слова: ИТ-субъект, ИТ-продукт, ИТ-проект, риск, комплаенс-риск, комплаенс-последствие.

Для цитирования:
Николаенко В.С. (2024). Комплаенс-риски эксплуатации ИТ-продуктов. *Стратегические решения и риск-менеджмент,* 15(4): 360–367. DOI: 10.17747/2618-947X-2024-4-360-367.

Благодарности
Работа выполнена в рамках государственного задания «Наука», проект FEWM-2023-0013.

Compliance-risks in the operation of IT products

V.S. Nikolaenko[1, 2, 3]
[1] Tomsk State University of Control Systems and Radioelectronics (Tomsk, Russia)
[2] Tomsk Polytechnic University (Tomsk, Russia)
[3] Siberian State Medical University (Tomsk, Russia)

Abstract
The article discusses compliance risks that can arise during the operation of IT products in the market and cause unacceptable damage to IT organisations. To achieve this goal, the author of this article conducted a study of civil, administrative and criminal judicial practice, where one of the parties was an IT company (OKVED 62), including disputes related to the infringement of exclusive rights to IT products. Based on the research conducted, 12 compliance risks were identified, of which 6 were civil, 1 was administrative and 5 were criminal. An analysis of judicial practice has shown that the withdrawal, distribution and operation of IT products on the market without taking into account these requirements exposes IT companies to civil, administrative and/or criminal liability. In addition, as part of the work carried out, the dynamics of criminal offences in the field of computer information was analysed, where it was found that in the period 2022-2023. The increase in offences related to unauthorised access to electronic devices rose from 9,308 to 36,788 crimes (an increase of 74.6%). The results of the study highlited the urgent need for IT stakeholdes to develop effective and efficient preventive measures to influence identified compliance risks. For example, the development of measures related to the review of requirements for documentary support of IT projects, the form and content of IT products, and ways of protecting computer information.
Keywords: IT-subject, IT-product, IT-project, risk, compliance-risk, compliance-consequence.

For citation:
Nikolaenko V.S. (2024). Compliance-risks in the operation of IT products. *Strategic Decisions and Risk Management,* 15(4): 360-367. DOI: 10.17747/2618-947X-2024-4-360-367. (In Russ.)

Acnowledgements
The work was carried out within the framework of the state task «Science», project FEWM-2023-0013.

运营 IT 产品的合规风险

V.S. Nikolaenko[1, 2, 3]
[1] 托木斯克国立系统管理与无线电电子大学(俄罗斯，托木斯克)
[2] 托木斯克理工大学 (俄罗斯，托木斯克)
[3] 西伯利亚国立医科大学 (俄罗斯，托木斯克)

简介
文章讨论了IT产品在市场运作过程中可能出现的合规风险，这些风险会对IT 产品造成不可接受的损害。为了实现这一目标，本文作者对民事、行政和刑事法院的实践进行了研究，其中一方当事人是信息技术主体（全俄罗斯经济活动分类手册62），包括研究与侵犯信息技术产品专有权有关的纠纷。根据所进行的研究，确定了 12 项合规风险，即 6 项民事风险、1 项行政风险和 5 项刑事风险。对司法实践的分析表明，在不考虑这些要求的情况下在市场上生产、销售和运营信息技术产品，会使信息技术主体面临民事、行政和/或刑事责任的威胁。此外，正在进行的工作分析了计算机信息领域刑事犯罪的趋势，发现在 2022 年至 2023 年期间，与未经授权访问电子设备有关的犯罪案件从 9 308 起增加到 36 788 起（增加了 74.6%）。研究结果表明，信息技术主体迫切需要制定切实有效的预防措施，以应对已发现的合规风险：例如，制定与核实信息技术项目文件支持要求、信息技术产品的形式和内容以及保护计算机信息的方法有关的措施。
关键词: IT 实体、IT 产品、IT 项目、风险、合规风险、合规后果。

供引用:
Nikolaenko V.S. (2024). 运营 IT 产品的合规风险。战略决策和风险管理, 15(4): 360–367. DOI: 10.17747/2618-947X-2024-4-360-367. (俄文)

致谢
这项工作是在国家任务 "科学 "的框架内进行的, FEWM-2023-0013项目。

Введение
Анализ бизнес-деятельности 495 ИТ-субъектов Томской области (ОКВЭД 62) показал, что во время создания ИТ-продуктов в рамках ИТ-проектов могут материализоваться порядка 170 универсальных рисков [Nikolaenko, Sidorov, 2023]. Углубленное изучение природы этих рисков позволило распределить их на четыре группы: коммерческие риски (3%), проектные риски (33%), риски внешней среды (37%) и комплаенс-риски (27%)[1]. Кроме того, было установлено, что наступление одного комплаенс-риска причиняет материальный ущерб ИТ-субъектам в 277 тыс. руб. в среднем. Если во время выполнения ИТ-проекта наступают два комплаенс-риска, то ущерб увеличивается до 554 тыс. руб., если три – до 831 тыс. руб. и т.д.

Под универсальными рисками в настоящей статье будут пониматься вероятные события, актуальные для ИТ-проектов независимо от их масштабов, сложности, длительности, типов, концепций создания ИТ-продуктов и численности участников [Paladino et al., 2009; Chapman, 2011; Aven, 2012; Brandas et al., 2012; Lee et al., 2013; De Baker et al., 2014; Mishra et al., 2014; Wieczorek-Kosmala, 2014; Beer et al., 2015; Luckmann, 2015]. Под комплаенс-рисками будут пониматься вероятные события, связанные с нарушением норм действующего законодательства, требований национальных стандартов и кодексов поведения, влекущие юридические последствия [Николаенко, 2024а].

Время актуализации 170 рисков в рамках проведенного исследования было ограничено следующими фазами жизненного цикла ИТ-проекта: формирование требований; разработка концепции автоматизированной системы; разработка технического задания (далее – ТЗ); разработка эскизного проекта; разработка технического проекта; разработка рабочей документации[2, 3]. Комплаенс-риски для фаз «ввод в действие» и «сопровождение» в силу поставленных целей исследования не определялись. Однако важно отметить, что информация о рисках, которые могут материализоваться во время данных этапов и повлечь наступление комплаенс-последствий, очень важна для ИТ-субъектов, которые планируют выводить, распространять и эксплуатировать ИТ-продукты на рынке.

В качестве подтверждения сказанного можно привести примеры, где предметом спора стали исключительные права на созданные ИТ-продукты. Например, в деле № А83-6393/2023[4] ООО «1С» просило суд взыскать компенсацию за нарушение исключительных прав в размере 268 тыс. руб. В деле № А81-11865/2022 ООО[5] «1С» и ООО «1С-Софт» требовало взыскать с АО «Партнер» 4,7 млн руб. В деле № А50-4247/2023[6] ООО «1С» обратилось в суд с требованием взыскать компенсацию в размере 684 тыс. руб. за незаконное использование ИТ-продуктов. В деле № А36-7440/2022[7] ООО «1С» просило суд защитить исключительные права на ИТ-продукты, принадлежащие ООО «1С», и взыскать с нарушителя 50 тыс. руб. Аналогичные требования зафиксированы в делах № А35-7078/2022[8] и № А08-16/2022[9]. В деле № А29-10372/2022[10] ООО «1С» просило суд о взыскании компенсации за незаконное использование ИТ-продуктов в размере 342 тыс. руб. В деле № А14-13243/2022[11] ООО «1С» и ООО «1С-Софт» требовали от ООО «СпецТех-Строй»

[1] Николаенко В. (2023). Безупречный риск-менеджмент: учеб. пособие. Томск, Изд-во ТУСУР.
[2] ГОСТ Р 59793-2021 (2020). Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Москва, Стандартинформ.
[3] ГОСТ Р 57102-2016/ISO/IEC TR 24748-2:2011 (2016). Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Ч. 2. Руководство по применению ИСО/МЭК 15288. Москва, Стандартинформ.
[4] Решение Арбитражного суда Республики Крым по делу № А83-6393/2023 от 18.09.2023. https://clck.ru/36cnZT.
[5] Решение Арбитражного суда Ямало-Ненецкого автономного округа по делу № А81-11865/2022 от 13.08.2023. https://clck.ru/36cpoK.
[6] Решение Арбитражного суда Пермского края по делу № А50-4247/2023 от 27.07.2023. https://clck.ru/36cpzX.
[7] Решение Арбитражного суда Липецкой области по делу № А36-7440/2022 от 13.06.2023. https://clck.ru/36cq88.
[8] Решение Арбитражного суда Курской области по делу № А35-7078/2022 от 13.03.2023. https://clck.ru/36d5KQ.
[9] Решение Арбитражного суда Белгородской области по делу № А08-16/2022 от 07.11.2022. https://clck.ru/36d7n5.
[10] Решение Арбитражного суда Курской области по делу № А29-10372/2022 от 30.12.2022. https://clck.ru/36d5W7.
[11] Решение Арбитражного суда Воронежской области по делу № А14-13243/2022 от 07.11.2022. https://clck.ru/36d7f5.

компенсацию за незаконное использование ИТ-продуктов в размере 2,4 млн руб.

Анализ судебной практики также показывает, что нередки случаи, когда нарушение исключительных прав трансформируется в уголовную ответственность. Наглядным примером является дело № 1-209/2022[12], где подсудимый без соответствующего разрешения правообладателя ООО «1С-Софт» скопировал на USB-носитель файл ИТ-продукта и осуществил множество незаконных установок, извлекая при этом коммерческую выгоду. Своими преступными действиями подсудимый нарушил конституционное право правообладателя на охрану интеллектуальной собственности, предусмотренное статьей 44 части 1 Конституции РФ[13], и причинил ему ущерб на сумму в размере 4,2 млн руб.

На основании сказанного можно заключить, что целью настоящей статьи является идентификация комплаенс-рисков, которые могут материализоваться во время эксплуатации ИТ-продуктов на рынке. Важно отметить, что в соответствии с условиями статьи 17 Федерального закона «Об информации, информационных технологиях и о защите информации» № 149-ФЗ[14] (далее – Закон № 149-ФЗ) правонарушения в сфере информационных технологий влекут дисциплинарную, гражданско-правовую, административную и (или) уголовную ответственность. В связи с этим для достижения поставленной цели было проведено исследование судебной практики, где предмет спора был связан с нарушением прав на ИТ-продукты либо где одной из сторон являлся ИТ-субъект (ОКВЭД 62).

1. Гражданско-правовые риски

Анализ арбитражной судебной практики показал, что во время эксплуатации ИТ-продуктов, как правило, наступают рисковые события двух видов: риски, связанные с качеством полученных ИТ-результатов выполненных работ (оказанных ИТ-услуг, поставленных ИТ-товаров), и риски, сопряженные с исключительными правами на результаты интеллектуальной деятельности (далее – РИД). В силу статьи 1261 ГК РФ[15] ИТ-продукт является РИД [Кузнецова и др., 2022]. Рассмотрим содержание этих комплаенс-рисков подробнее.

Риск выявления недостатков при использовании результата выполненной работы (оказанной услуги, поставленного товара). Под недостатком работы (услуги, товара) законодатель понимает любое несоответствие обязательным требованиям законов, национальных стандартов, условиям контракта и др. [Гаязов, 2022]. Например, если ИТ-продукт не отвечает заявленным требованиям, то он приобретает статус некачественного, что может повлечь наступление негативных комплаенс-последствий как для стороны подрядчика (исполнителя, поставщика), так и для стороны заказчика. В частности, если будет установлено, что для устранения дефектов требуются значительные затраты либо характер недостатков таков, что дефекты обнаруживаются повторно, то заказчик (покупатель) имеет право потребовать возвращения ему ранее уплаченной денежной суммы [Михайленко, Ковалева, 2021]. Стоит отметить, что в работе [Николаенко, 2024b] отмечается, что ИТ-продукт является сложным правовым объектом, который состоит из двух частей – ИТ-услуги и/или РИД (программы для ЭВМ).

Показательным примером выявления недостатков во время эксплуатации ИТ-продукта является дело № А45-15497/2020[16], где между ООО «Ера» (подрядчик) и ООО «Смартмедиа» (заказчик) был заключен контракт, в рамках которого подрядчик был обязан выполнить, а заказчик – оплатить работы по созданию мобильного приложения Boom Boom на платформах Android и iOS. В ходе «сопровождения» созданного ИТ-продукта заказчик выявил большое количество программных недостатков и потребовал от подрядчика переделать работу. Подрядчик отказал в выполнении данного требования. Для определения характера недостатков суд назначил экспертизу, которая установила, что результат выполненных работ частично соответствует условиям контракта, является некачественным и требует устранения выявленных дефектов. По итогу суд принял решение взыскать с ООО «Ера» 133,7 тыс. руб.

Риск нарушения авторских прав. Если лица изготавливают, распространяют и эксплуатируют ИТ-продукты без разрешения правообладателей, то данные программы признаются нелицензионными (контрафактными) [Копылов, 2019]. Использование подобных ИТ-продуктов запрещено и влечет для юридических лиц наступление гражданско-правовой либо административной ответственности, а для физических лиц – вплоть до уголовной ответственности.

Последствиями в случае наступления риска нарушения авторских прав могут быть запрет правообладателя использовать РИД с последующим взысканием убытков (компенсации) [Котовщиков, 2017]. Помимо гражданско-правовых последствий для субъекта, который нарушил права на РИД, возможны и более тяжкие комплаенс-последствия, например если субъект, стремясь извлечь доход, осуществил ввоз, продажу, сдачу в прокат контрафактных произведений либо на экземплярах произведений указал ложную информацию об обладателях авторских прав. Если факт совершения такого деяния будет установлен, то субъект будет привлечен к административной ответственности, предусмотренной статьей 7.12 КоАП РФ[17].

В качестве примера можно привести дело № 5–1637/2021[18], где правонарушитель незаконно эксплуатировал объекты авторского права в предпринимательской деятельности, а именно использовал контрафактные ИТ-продукты для приставок Sony PlayStation 4 Pro. Суд признал правонарушителя виновным и назначил наказание в виде административного штрафа 15 тыс. руб. без конфискации имущества.

Важно отметить, что тяжесть комплаенс-последствий будет существеннее, если субъект присвоит себе авторство (плагиат) и своими действиями будет причинять автору или

[12] Приговор Пролетарского районного суда г. Саранска Республики Мордовия по делу № 1-209/2022 от 07.09.2022. https://clck.ru/36eUWo.
[13] Конституция Российской Федерации. https://clck.ru/MsKLk.
[14] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. https://clck.ru/ggWjK.
[15] Гражданский кодекс Российской Федерации (ГК РФ). Комментарий к последним изменениям (2019). Москва, АБАК.
[16] Решение Арбитражного суда Новосибирской области по делу № А45-15497/2020 от 24.03.2022. https://clck.ru/36d7VV.
[17] Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) https://clck.ru/MsKtY.
[18] Постановление Промышленного районного суда г. Ставрополя по делу № 5-1637/2021 от 03.06.2021. https://clck.ru/36eUaL.

правообладателю материальный ущерб. В этом случае субъект может быть привлечен к уголовной ответственности, предусмотренной статьей 146 УК РФ[19]. Например, в деле № 1-108/2020[20] подсудимый нарушил исключительные права правообладателя ООО «1С» и причинил имущественный вред в размере 545,4 тыс. руб.

Риск того, что правообладатель запретит использовать РИД. Согласно статье 1252 ГК РФ, если субъект нарушает права на РИД, то правообладатель имеет возможность пресечь противоправные действия в форме прямого запрета. В качестве примера наступления такого риска следует рассмотреть дело № А53-23110/22[21], где ООО «Система-1» попросило суд запретить ФГБОУ ВО «РГУПС» неправомерное использование ИТ-продукта LabWagon. Изучив материалы дела, суд отказал в заявленных требованиях, так как пришел к выводу, что работник ООО «Система-1» является автором LabWagon, но не правообладателем. Судом было установлено, что этот работник создал спорный ИТ-продукт в рамках служебного задания, когда он состоял в трудовых отношениях с ФГБОУ ВО «РГУПС».

Риск взыскания правообладателем убытков (компенсации) за нарушение прав на РИД. Помимо прямого запрета по пресечению действий, нарушающих права на РИД, правообладателю предоставляется возможность взыскать с субъекта причиненный ущерб в форме возмещения убытков либо выплаты компенсации в пределах от 10 тыс. до 5 млн руб. [Шорохов, 2020].

Показательным примером материализации рассматриваемого риска является дело № А50-17729/2022[22], где правообладатель ООО «1С», установив факт незаконного использования своего ИТ-продукта, потребовал суд взыскать с ИП Языковой Г.Л. компенсацию в размере 400 тыс. руб.

Стоит отметить, что на практике также распространены случаи нарушения условий лицензионных договоров. Так, в деле № А67-8506/2018[23] ООО «САБ» просило суд взыскать с НП «Байкал-Тендер» задолженность по лицензионному договору в размере 3,5 млн руб.

Риск невозможности признания исключительного права на РИД за правообладателем. Несоблюдение правил создания РИД, например в рамках трудовых отношений между работодателем и работником, может привести к негативному сценарию, когда работодатель не может доказать, что он является правообладателем [Заидова, 2021]. Согласно статье 1295 ГК РФ исключительное право на служебное произведение, созданное работником в пределах установленных трудовых обязанностей, принадлежит работодателю.

В качестве примера материализации рассматриваемого риска следует привести дело № А40-90889/21-134-529[24], где АО «ВИСТ Групп» просило суд запретить использование ИТ-продукта ALTAN. Обосновывая свои требования, АО «ВИСТ Групп» ссылалось на то, что ИТ-продукт разработан его бывшими работниками в рамках служебных обязанностей. Рассмотрев материалы дела, суд отказал в удовлетворении заявленных требований, указав, что для установления факта того, что исключительное права на программу ALTAN принадлежат АО «ВИСТ Групп», необходимо подтвердить факт выдачи работникам служебного задания. Документально выдача служебного задания не была подтверждена, из чего суд заключил, что созданный ИТ-продукт не является служебным произведением, поэтому АО «ВИСТ Групп» не является правообладателем программы ALTAN.

Риск создания нежелательного производного произведения. Согласно статье 1270 ГК РФ переработка (модификация) ИТ-продуктов может привести к созданию производного произведения, которое является самостоятельным объектом авторского права [Бескодарова, 2020]. Данное обстоятельство может привести к нежелательному спору. В качестве примера подобного конфликта следует привести дело № А56-38522/2020[25], где ООО «Нмаркет.ПРО Рус» (истец) просило суд солидарно взыскать с владельцев сайта panpartner.ru компенсацию в размере 2 млн руб. В обоснование своих требований истец заявил, что программная часть сайта «Поисковый модуль» является его ИТ-продуктом. Назначенные судом эксперты пришли к выводу, что общий объем кода поискового модуля составляет 2669 строк, из которых 589 строк (22%) используются сайтом без изменений, а 1522 строки (57%) изменены частично. На основании заключения экспертов суд пришел к выводу, что владельцы сайта незаконно модифицировали поисковой модуль, создав тем самым нежелательное производное произведение.

2. Административные риски

Если во время создания и последующей эксплуатации ИТ-продуктов субъект нарушает требования в области защиты информации, например если он использует несертифицированные информационные системы, базы данных и другие средства защиты информации, то данный субъект может быть привлечен к административной ответственности, предусмотренной статьей 13.12 КоАП РФ.

В соответствии со статьей 21 Закона № 149-ФЗ защите подлежит любая информация, в том числе и компьютерная, неправомерное обращение с которой может нанести ущерб ее владельцу. Элиминирование данной угрозы осуществляется за счет применения средств защиты: например, ИТ-субъектам необходимо получение специальных лицензий, позволяющих осуществлять деятельность в области защиты информации.

Наглядным примером наступления риска, связанного с нарушением требований правил защиты информации, является дело № 5-300/2015[26]. Из материалов дела следует, что во время проверки ООО «Инфотелеком» нарушило требование в части обязательного наличия в штате квалифицированного персонала. Этот факт стал основанием для привлечения ИТ-субъекта к административной ответственности.

[19] Уголовный кодекс Российской Федерации (УК РФ) от 13.06.1996. № 63-ФЗ. https://clck.ru/ggWjK.
[20] Приговор Шпаковского районного суда Ставропольского края по делу № 1-108/2020 от 24.09.2020. //sudact.ru/regular/doc/Tg3F5jz1VEox/.
[21] Решение Арбитражного суда Ростовской области по делу № А53-23110/22 от 07.06.2023. https://clck.ru/36cr8y .
[22] Решение Арбитражного суда Пермского края по делу № А50-17729/2022 от 28.12.2022. https://clck.ru/36d5id.
[23] Решение Арбитражного суда Томской области по делу № А67-8506/2018 от 15.11.2018. https://clck.ru/3957JU.
[24] Решение Арбитражного суда города Москвы по делу № А40-90889/21-134-529 от 05.10.2023. https://clck.ru/36cmjw.
[25] Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области по делу № А56-38522/2020 от 14.04.2023. https://clck.ru/36d4mB.
[26] Постановление Советского районного суда г. Брянска по делу № 5-300/2015 от 29.05.2015. https://clck.ru/36ZdQH.

3. Уголовные риски

Согласно отчету о состоянии преступности в 2022 году в РФ было зарегистрировано 522,1 тыс. преступлений, совершенных с использованием ИТ или в сфере компьютерной информации,– 26,5% общего количество преступлений[27]. В 2023 году таких преступлений было зафиксировано уже 585,2 тыс.– 34,3% общего количества преступлений. Анализ судебной практики показал, что основные уголовные риски, которые материализуются во время эксплуатации ИТ-продуктов, относятся к сферам экономической деятельности и компьютерной информации. Рассмотрим их подробнее.

Риск хищения имущества путем ввода, удаления, блокирования, модификации компьютерной информации, оно же – мошенничество в сфере компьютерной информации (статья 159.6 УК РФ). В силу Закона № 149-ФЗ компьютерная информация – это информация, которая хранится в электронных устройствах и программах для ЭВМ. Данный риск характеризуется совершением деяния, которое связано с вводом, удалением, блокировкой, модификацией компьютерной информации с целью хищения чужого имущества или приобретения права на это имущество. По данным МВД РФ, в 2022 году в России было зарегистрировано 334 случая мошенничества в сфере компьютерной информации, в 2023 году – 417 таких преступлений.

В качестве примера незаконного ввода компьютерной информации можно привести дело № 1-422/2016[28], где подсудимый, используя мобильные телефоны и SIM-карты потерпевших, посредством направления SMS-сообщений неоднократно совершал незаконное списание денежных средств со счетов потерпевших.

Модификация компьютерной информации направлена на изменение сведений в электронном устройстве либо программе для ЭВМ. Примером незаконной модификации компьютерной информации является дело № 1-26/2017[29], где подсудимый, используя мобильный телефон потерпевшей, внес изменения в первоначальное состояние данных счета банковской карты.

Стоит отметить, что модификация компьютерной информации может быть осуществлена не только в электронных устройствах и программах для ЭВМ, но и в базах данных. Например, в деле № 1-30/2018[30] подсудимый внес заведомо ложные сведения об имеющихся излишне уплаченных юридическим лицом суммах НДС в базу данных «АИС-Налог».

Пример иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации представлен в деле № 1-139/2016[31], где подсудимая через личный кабинет программы «Президент-Сервис», используя логин и пароль, полученные преступным путем, похитила денежные средства, возвратив электронные проездные документы в кассах железнодорожного вокзала.

Отдельно стоит отметить дело № 1-48/2020[32]. Согласно материалам дела подсудимые и неустановленное следствием лицо, используя незаконно полученные пары «логин – пароль» вошли в личные кабинеты клиентов мультифункциональной бонусной платежной карты «Кукуруза» и совершили ряд операций по хищению электронных денежных средств.

Риск неправомерного доступа к компьютерной информации. Как правило, данный риск наступает в отношении компьютерной информации со специальным правовым режимом. В частности, к этой информации относятся персональные данные, сведения о личной, семейной, государственной, коммерческой, налоговой либо банковской тайне, конфиденциальная информация и др. По данным МВД РФ, в 2022 году в России было зарегистрировано 9308 случаев неправомерного доступа к компьютерной информации, в 2023 году – 36 788 таких преступлений.

В силу УК РФ неправомерным признается доступ к компьютерной информации субъекта, не обладающего правами на получение и работу с этой информацией, в отношении которой приняты специальные меры защиты по ограничению круга лиц, имеющих к ней доступ. Если субъект осуществляет незаконный либо неразрешенный доступ, то этот субъект может быть привлечен к уголовной ответственности, предусмотренной статьей 272 УК РФ.

Примером неправомерного доступа к компьютерной информации является дело № 1-190/2016[33]. Согласно материалам дела подсудимый в целях сбыта и получения прибыли от продажи контрафактных копий ИТ-продуктов (Компас-3D V16, CorelDRAW X6, Microsoft Windows 7 и Microsoft Office профессиональный плюс 2010) путем их установки совершил девять преступлений. Итоговая сумма материального ущерба, который причинил подсудимый правообладателям, составила 1,6 млн руб.

Примером модификации компьютерной информации является дело № 1-257/2023[34], где подсудимая, являясь специалистом офиса, через программу «1С Retail» осуществила неправомерный доступ и незаконно оформила SIM-карты.

В качестве примера копирования компьютерной информации, то есть переноса информации на обособленный носитель при сохранении неизменной первоначальной информации, является дело № 1-457/2022[35], где подсудимая осуществила копирование персональных данных собственников объектов недвижимости и передала их в чате коммуникационного сервиса мгновенного обмена сообщениями.

Риск создания, использования и распространения вредоносных компьютерных программ. Под вредоносными программами понимаются компьютерные вирусы, которые предназначены для несанкционированного уничтожения, блокирования, модификации и копирования компьютерной информации. Если субъект использует и распространяет вредоносные программы, то он может быть привлечен к уголов-

[27] ФКУ «Главный информационно-аналитический центр». https://clck.ru/395A4r.
[28] Приговор Рудничного районного суда г. Кемерово Кемеровской области делу № 1-422/2016 от 26.09.2016. https://clck.ru/395cv4.
[29] Приговор Братского городского суда Иркутской области по делу № 1-26/2017 от 22.09.2016. https://clck.ru/395d3Z.
[30] Приговор Ленинского районного суда по делу № 1-30/2018 от 11.04.2017. https://clck.ru/395dBV.
[31] Приговор Синарского районного суда г. Каменска-Уральского Свердловской области по делу № 1-139/2016 от 17.09.2016. https://clck.ru/395dKd.
[32] Приговор Куйбышевского районного суда г. Омска по делу № 1-48/2020 от 27.12.2019. https://clck.ru/395dPY.
[33] Приговор Северского городского суда Томской области по делу 1-190/2016 от 23.06.2016. https://clck.ru/36VDoX.
[34] Приговор Златоустовского городского суда Челябинской области по делу 1-257/2023 от 11.04.2023. https://clck.ru/36UcMi.
[35] Приговор Кузнецкого районного суда Пензенской области по делу № 1-457/2022 от 08.12.2022. https://clck.ru/36Ucs4.

ной ответственности, предусмотренной статьей 273 УК РФ. По данным МВД РФ, в 2022 году в России было зарегистрировано 200 случаев создания, использования и распространения вредоносных компьютерных программ (на 36,9% меньше по сравнению с 2021 годом), в 2023 году – 196 таких преступлений.

Примером копирования компьютерной информации с помощью компьютерного вируса является дело № 1-226/2023[36], где подсудимый с целью просмотра видеоизображений с камер видеонаблюдения и веб-камер персональных компьютеров пользователей сети Интернет использовал вирус и осуществил несанкционированное копирование с этих устройств.

В качестве примера нейтрализации средств защиты следует привести дело № 1-355/2023[37]. Под нейтрализацией средств защиты понимается негативное воздействие на технические, криптографические и другие средства с целью получения несанкционированного доступа к защищенной компьютерной информации. Согласно материалам дела подсудимый незаконно использовал вредоносную программу techsys.dll, для того чтобы нейтрализовать установленные правообладателем средства защиты.

Риск нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации. Согласно УК РФ ответственность за нарушения правил доступа и эксплуатации наступает, если субъект причиняет собственнику ущерб, сумма которого превышает 1 млн руб. В этом случае для субъекта может наступить уголовная ответственность, предусмотренная статьей 274 УК РФ.

Показательным примером наступления рассматриваемого риска является дело № 1-22/2021[38], где подсудимые и неустановленное следствием лицо разработали планы тайного хищения денежных средств из банкоматов на территории Красноярского края и незаконно проникли в банкоматы, нарушив правила их эксплуатации. Для этого они подключали ноутбук к диспенсеру банкомата и использовали вредоносные программы, что приводило к непрекращающейся выдаче банкоматами всех имеющихся денежных средств. В общей сложности подсудимые совершили четыре подключения и причинили ущерб собственникам, равный 17,5 млн руб.

Риск неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (далее – КИИ РФ). Согласно статье 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ[39] (далее – Закон 187-ФЗ) КИИ являются информационные системы субъектов КИИ. Для субъекта, который неправомерного воздействует на КИИ, может наступить уголовная ответственность, предусмотренная статьей 274.1 УК РФ.

Примером материализации риска является дело № 1-171/2023[40]. Исследование материалов дела показало, что подсудимые подключили услуги «Мобильный платеж» на абонентские номера ПАО «ВымпелКом», информационная инфраструктура которого является объектом КИИ РФ. Противоправные действия подсудимых нарушили целостность и актуальность компьютерной информации. Для локализации возникшей проблемы ПАО «ВымпелКом» было вынуждено приостановить работу сервиса MTopUp на территории РФ.

Заключение

В результате проведенного исследования было идентифицировано 12 комплаенс-рисков – 6 гражданско-правовых, 1 административный и 5 уголовных. Отдельно стоит отметить динамику роста уголовных преступлений, совершенных с использованием ИТ или в сфере компьютерной информации. В частности, в период 2022–2023 годов рост преступлений, связанных с неправомерным доступом к компьютерной информации и электронным устройствам, увеличился с 9308 до 36 788 случаев, то есть составил 74,6%.

Полученные результаты указывают на необходимость создания ИТ-субъектами результативных и эффективных превентивных мер воздействия на выявленные комплаенс-риски, например на соблюдение и реализацию требований, которые предъявляются к документальному сопровождению ИТ-проектов, форме и содержанию ИТ-продуктов, а также способам защиты компьютерной информации. Анализ судебной практики показал, что вывод, распространение и эксплуатация ИТ-продуктов на рынке без учета этих требований грозит для ИТ-субъектов наступлением нежелательных комплаенс-последствий.

Литература

Бескодарова В. (2020). Авторские договоры. *Синергия наук,* 45: 158–163.

Гаязов И.Р. (2022). К вопросу о модификации программ для ЭВМ. *Интернаука,* 22–6(245): 21–32.

Заидова Э.Б. (2021). Проблемы эффективности модели предоставления исключительных прав на программу для ЭВМ через авторский заказ. *Научные исследования XXI века,* 1(9): 331–334.

Копылов А.Ю. (2019). Основные квалификационные признаки произведения как объекта авторских прав. *Вопросы российского и международного права,* 9(10–1): 106–112.

Котовщиков А.В. (2017). Программы для ЭВМ в системе объектов исключительных прав. В: *Актуальные проблемы гражданского права и гражданского судопроизводства:* 75–78.

Кузнецова К.О., Чернова Е.А., Майер В.Р., Гарифуллин Р.Ф. (2022). Информационный менеджмент. *Интернаука,* 40–4(263): 54–55.

Михайленко К.А., Ковалева К.А. (2021). Обзор и анализ развития программного обеспечения. В: *Актуальные проблемы науки и образования в условиях современных вызовов:* сборник материалов II Международной научно-практической конференции: 52–55.

[36] Приговор Пролетарского районного суда г. Тула по делу № 1-226/2023 от 31.08.2023. https://clck.ru/36UeQA.
[37] Приговор Новоуренгойского городского суда Ямало-Ненецкого автономного округа по делу № 1-355/2023 от 27.09.2023. https://clck.ru/36UeHN.
[38] Приговор Советского районного суда г. Красноярск по делу № 1-22/2021 от 03.06.2021. https://clck.ru/36Uezy.
[39] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». https://clck.ru/33sX2n.
[40] Приговор Вахитовского районного суда г. Казань Республики Татарстан по делу № 1-171/2023 от 02.11.2022. https://clck.ru/36UdEr.

Николаенко В. (2024a). ИТ-продукт: уточнение понятия. *Векторы благополучия: экономика и социум,* 52(3): 136–145.

Николаенко В. (2024b). Комплаенс-особенности создания ИТ-продуктов в рамках выполнения ИТ-проектов. *Проблемы анализа риска,* 21(5): 97–107.

Шорохов Д.А. (2020). Выбор программного обеспечения для создания веб-сайта. *Актуальные научные исследования в современном мире,* 7–1(63): 219–226.

Aven T. (2012). The risk concept – Historical and recent development trends. *Reliability Engineering and System Safety,* 99: 33–44.

Beer M., Wolf T., Garizy T.Z. (2015). Systemic risk in IT portfolios – An integrated quantification approach. In: *International conference on information systems: Exploring the information frontier:* 1–18.

Brandas C., Didraga O., Bibu N. (2012). Study on risk approaches in software development project. *Informatica Economica,* 16(3): 148−157.

Chapman R. (2011). *Simple tools and techniques for enterprise risk management.* Chichester, Wiley.

De Baker K., Boonstra A., Wortmann H. (2014). The communicative effect of risk identification on project success. *Project Organisation and Management,* 6: 138−156.

Lee O.-K.D., Baby D.V. (2013). Managing dynamic risks in global IT projects: Agile risk-management using the principles of service-oriented architecture. *International Journal of Information Technology & Decision Making,* 12: 1121−1150.

Luckmann J.A. (2015). Positive risk management: Hidden wealth in surface mining. *Journal of the Southern African Institute of Mining and Metallurgy,* 115: 1027–1034.

Mishra A., Das S., Murray J. (2014). Managing risk in government information technology projects: Does process maturity matter? *Production and Operations Management,* 24(3): 365–368.

Nikolaenko V., Sidorov A. (2023). Analysis of 105 IT project risks. *Journal of Risk and Financial Management,* 16(1): 33. DOI: https://doi.org/10.3390/jrfm16010033.

Paladino B., Cuy L., Frigo M. (2009). Missed opportunities in performance and enterprise risk management. *Journal of Corporate Accounting & Finance,* 20(3): 43–51.

Wieczorek-Kosmala M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies,* 19(2): 133–159.

References

Beskodarova V.S. (2020). Author's agreements. *Synergy of Sciences,* 45: 158-163. (In Russ.)

Gayazov I.R. (2022). On the issue of modifying computer programs. *Internauka,* 22-6(245): 21-32. (In Russ.)

Zaidova E.B. (2021). Problems of the efficiency model of granting real rights to a computer program through an author's order. *Scientific Research of the XXI Century,* 1(9): 331-334. (In Russ.)

Kopylov A.Yu. (2019). Basic qualifying characteristics of works as an object of copyright. *Issues of Russian and International Law,* 9(10-1): 106-112. (In Russ.)

Kotovshchikov A.V. (2017). Computer programs in the system of objects of object rights. In: *Current problems of graphic law and graphic legal proceedings:* 75-78. (In Russ.)

Kuznetsova K.O., Chernova E.A., Mayer V.R., Garifullin R.F. (2022). Information management. *Interscience,* 40-4(263): 54-55. (In Russ.)

Mikhailenko K.A., Kovaleva K.A. (2021). Review and analysis of software development. In: *Current problems of science and education in the context of modern challenges:* Collection of materials of the II International Scientific and Practical Conference: 52-55. (In Russ.)

Nikolaenko V.S. (2024). IT-product: Clarification of the concept. *Journal of Wellbeing Technologies,* 52(3): 136-145. (In Russ.)

Nikolaenko V.S. (2024). Compliance-features of creating IT-products within the framework of IT-project. *Issues of Risk Analysis,* 21(5): 97-107. (In Russ.)

Shorokhov D.A. (2020). Selection of software for creating a website. *Current Scientific Research in the Modern World,* 7-1(63): 219-226. (In Russ.)

Aven T. (2012). The risk concept - Historical and recent development trends. *Reliability Engineering and System Safety,* 99: 33-44.

Beer M., Wolf T., Garizy T.Z. (2015). Systemic risk in IT portfolios - An integrated quantification approach. In: *Exploring the Information Frontier: International conference on information systems:* 1-18.

Brandas C., Didraga O., Bibu N. (2012). Study on risk approaches in software development project. *Informatica Economica,* 16(3): 148-157.

Chapman R. (2011). *Simple tools and techniques for enterprise risk management.* Chichester, Wiley.

De Baker K., Boonstra A., Wortmann H. (2014). The communicative effect of risk identification on project success. *Project Organisation and Management,* 6: 138-156.

Lee O.-K.D., Baby D.V. (2013). Managing dynamic risks in global IT projects: Agile risk-management using the principles of service-oriented architecture. *International Journal of Information Technology & Decision Making,* 12: 1121-1150.

Luckmann J. A. (2015). Positive risk management: Hidden wealth in surface mining. *Journal of the Southern African Institute of Mining and Metallurgy,* 115: 1027-1034.

Mishra A., Das S., Murray J. (2014). Managing risk in government information technology projects: Does process maturity matter? *Production and Operations Management,* 24(3): 365-368.

Nikolaenko V., Sidorov A. (2023). Analysis of 105 IT project risks. *Journal of Risk and Financial Management,* 16(1): 33. DOI: https://doi.org/10.3390/jrfm16010033.

Paladino B., Cuy L., Frigo M. (2009). Missed opportunities in performance and enterprise risk management. *Journal of Corporate Accounting & Finance,* 20(3): 43-51.

Wieczorek-Kosmala M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies,* 19(2): 133-159.

Информация об авторе

Валентин Сергеевич Николаенко

Кандидат экономических наук, доцент кафедры автоматизации обработки информации Томского государственного университета систем управления и радиоэлектроники (Томск, Россия); доцент Бизнес-школы Томского политехнического университета (Томск, Россия); доцент кафедры экономики, социологии, политологии и права Сибирского государственного медицинского университета (Томск, Россия). ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

Область научных интересов: риск-менеджмент, национальная безопасность, экономическая безопасность, информационное право и защита интеллектуальной собственности, гражданское право, управление проектами.

valentin.s.nikolaenko@tusur.ru

About the author

Valentin S. Nikolaenko

Candidate of economic sciences, associate professor at the Department of Automation of Information Processing, Tomsk State University of Control Systems and Radioelectronics (Tomsk, Russia); associate professor at the Business School, Tomsk Polytechnic University (Tomsk, Russia); associate professor at the Department of Economics, Sociology, Political Science and Law, Siberian State Medical University (Tomsk, Russia). ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

Research interests: risk-management, national security, economic security, information law and intellectual property protection, civil law, project management.

valentin.s.nikolaenko@tusur.ru

作者信息

Valentin S. Nikolaenko

经济学副博士，托姆斯克国立系统管理与无线电电子大学（（俄罗斯，托木斯克）信息处理自动化系教授；　托木斯克理工大学（俄罗斯，托木斯克）商学院副教授；西伯利亚国立医科大学（俄罗斯，托木斯克）经济学、社会学、政治学和法学系副教授。ORCID: 0000-0002-1990-4443; Web of Science Researcher ID: J-8521-2015; SPIN: 9301-1835; Author ID: 745788; IRID: 283767926; Scopus Author ID: 57193434445.

科学兴趣领域: 风险管理、国家安全、经济安全、信息法和知识产权保护、民法、项目管理。

valentin.s.nikolaenko@tusur.ru

Статья поступила в редакцию 21.11.2024; после рецензирования 18.12.2024 принята к публикации 22.12.2024. Автор прочитал и одобрил окончательный вариант рукописи.

The article was submitted on 21.11.2024; revised on 18.12.2024 and accepted for publication on 22.12.2024. The author read and approved the final version of the manuscript.

文章于 21.11.2024 提交给编辑。文章于 18.12.2024 已审稿。之后于 22.12.2024 接受发表。作者已经阅读并批准了手稿的最终版本。