ОЦЕНКА СТЕПЕНИ ВЛИЯНИЯ GENERAL DATA PROTECTION REGULATION НА БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Лившиц И.И.[1]

Аннотация

Целью исследования *является анализ существующих требований по обеспечению безопасности персональных данных и оценка степени влияния этих требований на безопасность жизнедеятельности предприятий в Российской Федерации.*

Метод исследования: *исследуется проблема обеспечения безопасности персональных данных в соответствии с требованиями Федерального закона Российской Федерации ФЗ-152 и международного регламента General Data Protection Regulation. Анализируются возможные риски прерывания нормальной деятельности предприятий в Российской Федерации в силу нарушения указанных требований по защите персональных данных и наложения существенных штрафов международными регуляторами. Оцениваются численные зависимости между размером штрафов за нарушения установленных требований, в том числе General Data Protection Regulation и стоимостью создания эффективной системы защиты персональных данных. Получены оценки допустимой степени влияния требований General Data Protection Regulation на безопасность предприятий в Российской Федерации.*

Результат исследования: *выполнено исследование и сопоставление возможных штрафов за нарушение соответствия требованиям Федерального закона Российской Федерации ФЗ-152 и международного регламента General Data Protection Regulation. Получены оценки рисков санкций за нарушение установленных требований по защите персональных данных. Выполнен анализ стоимости подготовки системы защиты персональных данных на соответствие требованиям регламента General Data Protection Regulation. На основе полученных данных представлены примеры расчета степени зрелости системы защиты – на основании соотношений доли бюджета, выделяемой на обеспечение безопасности по отношению к стоимости создания эффективной системы защиты персональных данных и на основании соотношения размера штрафов за нарушение установленных требований. Показана важность учета затрат на обеспечение безопасности персональных данных для обеспечения безопасности деятельности предприятий в Российской Федерации с учетом требований General Data Protection Regulation.*

Ключевые слова: *персональные данные, оценка риска, бюджет, ущерб, Федеральный закон, угроза, степень зрелости, система, оценка соответствия.*

DOI: 10.21681/2311-3456-2020-04-66-75

Введение

Общий Регламент о Защите Данных Европейского Союза (далее – GDPR) вступил в силу 25 мая 2018 г. [1]. Кратко, Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных (далее – ПДн) и о свободном обращении таких данных, состоит из двух частей, преамбулы и основной части [2]. Преамбула включает 173 положения, разъясняющих состав статей основной части, а основная часть представлена 11 главами и 99 статьями [3]. GDPR регулирует обработку ПДн граждан и резидентов ЕС, но, тем не менее, этот Регламент важен для российских предприятий, которые выступают в роли операторов ПДн, прежде всего по причине того, что GDPR имеет уникальное экстерриториальное свойство [4]. Это означает, что под его воздействие попадают операторы ПДн, обрабатывающие ПДн граждан и резидентов ЕС, в не зависимости от их территориального расположения. GDPR оказывает явное воздействие на операторов ПДн, например, на операторов, владеющих интернет-сайтами, которые посещают граждане ЕС [5, 6]. С учетом имеющейся практики защиты ПДн, организации в Российской Федерации выполняют в минимальном объеме требования Федерального закона № 152-ФЗ (далее – ФЗ-152) и ряда подзаконных актов (ФСТЭК России, ФСБ России), но они могут быть недостаточными в целях соответствия GDPR. Это обстоятельство особенно актуально, если рассматриваются российские предприятия, являющиеся контрагентами зарубежных организаций: филиалами, деловыми представительствами, партнерами и пр. [7, 8]. В этом случае возникает существенный риск не только прерывания деловой

1 Лившиц Илья Иосифович, доктор технических наук, доцент университета ИТМО, г. Санкт-Петербург, Россия. E-mail: Livshitz.il@yandex.ru

активности, но и значительные прямые финансовые потери при выявлении фактов нарушения установленных требований GDPR.

Постановка задачи

С учетом уже сложившейся в Российской Федерации практики выполнения проектов по обеспечению защиты ПДн, объективно существует методическая база ФСТЭК России в части, например, формирования моделей угроз по типовым шаблонам и выбора рекомендованных мер защиты [9, 10, 11]. Можно заметить, что вопросы надлежащей защиты ПДн рассматривались еще задолго до появления «профильного» закона 152-ФЗ [12, 13]. Кроме того, в современном законодательстве Российской Федерации определены не только требования информационной безопасности (ИБ), но и санкции за нарушения законодательства о ПДн. Следует отметить, что GDPR в целом устанавливает политику соответствия (Compliance [14, 15, 16]), и эта практика соответствия пока недостаточно распространена в Российской Федерации. Именно проблематика обеспечения соответствия и значительные финансовые штрафы являются мощными факторами влияния на лиц, принимающих решения (далее – ЛПР) крупнейших мировых компаний о внедрении мер обеспечения требований GDPR [17, 18, 19].

Однако для многих предприятий до сих пор остается проблемой принятие ЛПР мотивированного решения о создании обоснованной экономически эффективной системы защиты ПДн, а также о способах создания такой системы – самостоятельно или с помощью консультантов [20, 21, 22]. В настоящее время на рынке известно достаточно предложений о готовности создать «под ключ» системы защиты ПДн, а также обеспечить соответствие GDPR. Но остается неопределенным ряд вопросов – как оценивать текущий уровень обеспечения защиты ПДн? Какие экономические критерии финансового обеспечения проекта следует обеспечить? Какие риски следует предусмотреть и какие стратегии реагирования необходимо разработать?

Соответственно, не принятие во внимание многих вопросов может изначально привести к критическим нарушениям в процессе обеспечения соответствия GDPR, начиная от неверной оценки применимости, заканчивая попыткой дублирования элементов системы защиты ПДн, изначально спроектированной только под требования ФЗ-152 и ряда подзаконных актов (Постановление Правительства № 1119, Приказы ФСТЭК России и пр.). Следует учесть, что в российском законодательстве в области ПДн методы риск-менеджмента не упоминаются вовсе и отчасти GDPR является для многих предприятий новацией.

Постановка задачи сформирована как оценка степени экономического влияния GDPR на безопасность деятельности предприятий в Российской Федерации с целью получения оценки рисков соответствия при обеспечении новых законодательных требований.

Требования GDPR

В соответствии с GDPR Европейская Комиссия посредством оценки определяет постоянно обновляющийся список стран и международных организаций, гарантирующих соответствующий уровень защиты ПДн, и такие проверки проводятся не реже чем раз в четыре года [5]. В список включены Андорра, Аргентина, Израиль, Новая Зеландия, Швейцария, Япония, Уругвай, США, Канада, Фарерские острова, остров Джерси, остров Мэн. Российская Федерация в данном списке отсутствует, что означает явные ограничения передачи ПДн только на соответствующих гарантиях. Такой гарантией может выступать договор между «контролером» или «обработчиком» и субъектом ПДн (в терминах GDPR). Кроме того, для гарантии соответствия требованиям GDPR третьей страной, компетентные надзорные органы могут разрабатывать юридически обязывающие правила, исполнение которых дает гарантию соответствующего уровня защиты ПДн [23, 24].

За нарушение требований GDPR предусмотрены крупные штрафы, которые могут составлять до 20 миллионов евро или 4% годового оборота предприятия, в зависимости от того, что больше. Для контроля соблюдения GDPR операторами ПДн во всем мире была учреждена сеть надзорных органов под руководством Европейского Совета по защите данных [9]. По состоянию на 10 июня 2020 г. общая сумма штрафов за нарушение требований GDPR составляла более 150 млн. евро, при этом эта сумма не учитывает крупнейшие штрафы, наложенные на авиакомпанию British Airways (свыше 204 млн. евро) и сеть международных отелей Marriot International (свыше 110 млн. евро), поскольку окончательные суммы штрафов еще не согласованы [3].

Требования Федерального закона № 152-ФЗ

Основным документом, регулирующим обработку ПДн в Российской Федерации, является Федеральный закон «О персональных данных» (ФЗ-152). ФЗ-152 состоит из 6 глав, разделенных на 25 статей, и последние изменения и дополнения были внесены 24 апреля 2020 г. За нарушение ФЗ-152 предусмотрена ответственность в соответствии с ст. 13.11. Кодекса об административных правонарушениях Российской Федерации (далее – КоАП), также законодательство Российской Федерации предусматривает уголовную, гражданско-правовую и дисциплинарную ответственность. Статья 13.11. КоАП предусматривает административные штрафы для юридических лиц (с правками от 2 декабря 2019 года) до 75 тыс. руб. Более серьезное наказание следует за невыполнение требований при сборе ПДн и при использовании БД на территории Российской Федерации – от 1 до 6 млн. руб., а повторное нарушение – от 6 до 18 млн. руб. Дополнительно отметим, что ст. 24 ФЗ-152 предусматривает возмещение и морального вреда субъекту ПДн в случае нарушения его прав при обработке, при этом возмещение морального вреда осуществляется независимо от понесенных субъектом ПДн потерь. Сравнение штрафных санкций, предусмотренных GDPR и КоАП, сведено в единую таблицу (см. Табл. 1).

DOI: 10.21681/2311-3456-2020-04-66-75

Таблица 1

Сравнение штрафных санкций, предусмотренных GDPR и КоАП

Положение	GDPR	КоАП РФ для юр. лиц
Согласие на обработку ПДн ребенка	до 10 миллионов евро или 2% годового оборота предприятия, в зависимости от того, какая сумма больше	15 – 75 тыс. руб.
Обработка без идентификации		не применяется
Безопасность ПДн		25 – 50 тыс. руб.
Уведомление об утечке ПДн		не применяется
Ведение учета деятельности		не применяется
Назначение уполномоченных лиц		не применяется
Сертификация		не применяется
Соблюдение основных принципов обработки ПДн	до 20 миллионов евро или 4% годового оборота предприятия, в зависимости от того, какая сумма больше	предусмотрены штрафы за нарушение конкретных принципов
Публикация политики в отношении обработки ПДн		15 – 30 тыс. руб.
Законность обработки		15 – 30 тыс. руб.
Согласие субъекта на обработку ПДн		15 – 75 тыс. руб.
Обработка особых категорий ПДн		отдельно не рассматривается
Доступ субъекта к ПДн		20 – 40 тыс. руб.
Уточнение, блокировка и удаление ПДн в установленный срок		25 – 45 тыс. руб.
Трансграничная передача ПДн		отдельно не рассматривается
Требования уполномоченного органа		3 – 5 тыс. руб.
Требования законодательств государств-членов ЕС		не применяется
Локализация БД на территории РФ	не применяется	1 – 6 млн. руб. 6 – 18 млн руб. при повторном нарушении

Таблица 2

Стоимость услуги при внедрении GDPR

Услуга	Стоимость (ориентировочно)
Сертификация на 3 года	От 65 тыс. руб. (до 250 сотрудников)*
	От 250 тыс. руб. (от 260 сотрудников)
Разработка документации	От 300 тыс. руб.**
	От 170 тыс. руб.
Разработка плана внедрения GDPR	От 15 тыс. евро (100-500 сотрудников)***
Консалтинг по GDPR	От 300 евро/час

Услуга	Стоимость (ориентировочно)
Услуги представителя в ЕС	От 850 евро/год, не более 20 обращений субъектов ПДн, не более 10 обращений надзорных органов****
Обучение инспектора по защите данных	14 500 руб.*****

* https://www.iso-group.ru/uslugi/sertifikaty/gdrp
** https://acribia.ru/services/privacy
*** https://data-privacy-office.com/services/gdpr-roadmap-implementation
**** https://m.l-b.ru/services/legal_serv/gdpr
***** https://www.spbissa.ru/Learn/Gdpr

Стоимость подготовки системы защиты ПДн по требованиям GDPR

Из открытых источников известны примеры и стоимость услуг по созданию или приведению системы защиты ПДн в соответствие к требованиям GDPR (см. Табл. 2)

Основные промежуточные выводы из Табл. 1 и Табл.2:

1. В случае реализации риска выявления несоответствий только при проверках на соответствие требованиям ФЗ-152воздействие на бюджет предприятия оказывается низким, поскольку минимальные суммы штрафов оказываются кратно меньше стоимости работ, указанных в Табл. 2. Это означает, что затраты на выполнение требований ФЗ-152, в том числе затраты на внедрение мер защиты, могут быть максимально снижены, а риски санкций потенциальных несоответствий приняты. Такая стратегия наиболее часто применяется российскими операторами ПДн.
2. В случае реализации риска выявления несоответствий при проверках на соответствие требованиям GDPR воздействие на бюджет будет существенно выше, поскольку сумма штрафов может значительно превосходить затраты на создание корпоративной системы защиты ПДн. Это означает, что риски требуют обработки и необходимо создание эффективной системы защиты ПДн. Но, как следует из приведенных выше примеров исков против British Airways и Marriot International, даже крупнейшие компании мира и лидеры в своих сегментах рынка предпочитают экономить.

Расчет степени зрелости системы защиты ПДн

Рассмотрим примеры расчета оценки уровня защиты ПДн, принимая во внимания общие положения. Крайне важно принять во внимание, что степень зрелости систем защиты ПДн должна учитывать потенциал базовой системы ИБ, как правило, существующей на любом предприятии и упорно игнорируемой консультантами. В простейшем случае формула включает 2 переменные:

$$R_{GDPR} = C_{ITSM} \cdot L_{ITSM} \quad (1)$$

где:

R_{GDPR} – Оценка уровня защиты ПДн;

C_{ITSM} – Доля бюджета, выделяемого на общее обеспечение ИБ, в том числе, на приведение в соответствие требованиям защиты ПДн (GDPR);

L_{ITSM} – Степень зрелости существующей базовой системы ИБ.

Покажем на пример, как степень зрелости базовой системы (дискретная величина от 0 до 1 с шагом 0,25) и доля бюджета (процентная величина от 0% до 100% с шагом 10%) влияет на оценку уровня защиты ПДн (см. Табл. 3). В формуле (1) абсолютное значение бюджета исключено намеренно, чтобы был ясен замысел исследования и огромные суммы не мешали бы анализу. В принципе, в формуле (1) могут быть и иные переменные: финансовые (ROI, NPV) или дополнительные оценочные коэффициенты (временные, вероятностные, объектового охвата и пр.) или коэффициенты достоверности результата аудитов различной стороной (в соответствии с методиками ISO) [25, 26].

Графические результаты расчета по формуле (1) для всего диапазона значений переменных показаны на рис. 1.

Очевидна линейная зависимость оценки уровня защиты ПДн (R_{GDPR}) от степени зрелости существующей базовой системы ИБ предприятия (L_{ITSM}). В то же время явно следует, что даже при максимальной степени зрелости (L_{ITSM} = 1) предприятие не сможет «прыгнуть» выше доли бюджета (соответственно, при C_{ITSM} = 10% R_{GDPR} также будет 10% и далее аналогично). С другой стороны, для оценки потенциально достижимого показателя R_{GDPR} важное значение получает сопоставление кратности бюджета, выделяемого на срочное «приведение в соответствие» существующей системы ИБ. Например, даже при максимальном бюджете (C_{ITSM} = 100%) и одновременно при невысокой (отличной от нуля) степени зрелости (L_{ITSM} = 0,25) наилучший R_{GDPR} будет только 25%, что сопоставимо с показателем R_{GDPR} при (L_{ITSM} = 1) и кратно меньшим (в 3 раза) доли бюджета (C_{ITSM} = 30%). Этот факт весьма важен для ЛПР при общении с недобросовестными консультантами, обещающими «залить проблему деньгами». Расчеты убедительно говорят об обратном – гораздо выгоднее (экономически кратно выгоднее!) содержать существующую систему обеспечения ИБ в высокой степени «боеготовности», даже в условиях скромного финансирования.

DOI: 10.21681/2311-3456-2020-04-66-75

Таблица 3.

Расчета зрелости системы защиты ПДн

Доля бюджета C_{ITSM}, %	Оценка уровня защиты ПДн, RGDPR				
	Степень зрелости $L_{ITSM} = 0$	Степень зрелости $L_{ITSM} = 0,25$	Степень зрелости $L_{ITSM} = 0,5$	Степень зрелости $L_{ITSM} = 0,75$	Степень зрелости $L_{ITSM} = 1$
0	0	0	0	0	0
10	0	2,5	5	7,5	10
20	0	5	10	15	20
30	0	7,5	15	22,5	30
40	0	10	20	30	40
50	0	12,5	25	37,5	50
60	0	15	30	45	60
70	0	17,5	35	52,5	70
80	0	20	40	60	80
90	0	22,5	45	67,5	90
100	0	25	50	75	100

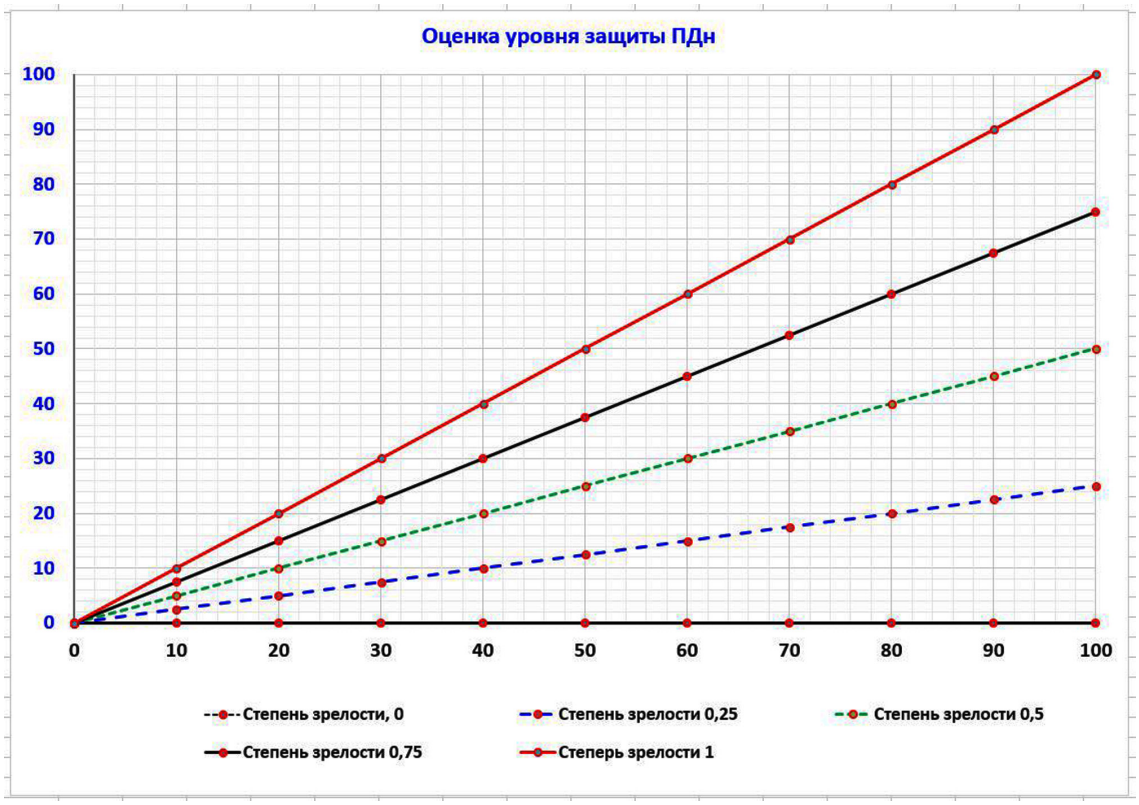

Рис. 1. Результаты расчета уровня защиты ПДн по Табл. 3

Данное исследование продолжим с учетом нового соотношений бюджета и потенциального ущерба (штрафов) за нарушение норм GDPR. Тогда формула (1) незначительно меняется для оценки зависимостей и принимает вид (2):

$$R_{GDPR} = Log_{10}(N_{GDPR}) \cdot L_{ITSM} \quad (2)$$

где:

R_{GDPR} – Оценка уровня защиты ПДн;

N_{GDPR} – Степень соотношения потенциальной доли бюджета, выделяемой на обеспечение ИБ, в том числе, на приведение в соответствие требованиям защиты ПДн (GDPR) и потенциального штрафа;

L_{ITSM} – Степень зрелости существующей базовой системы ИБ.

Покажем на пример, как степень зрелости базовой системы (дискретная величина от 0 до 1 с шагом 0,25) и соотношение потенциального доли бюджета, выделяемой на обеспечение ИБ, в том числе, на приведение в соответствие требованиям защиты ПДн (GDPR) и штрафа (дискретная величина от 0,1 до 0,0001) влияет на оценку уровня защиты ПДн (GDPR), см. Табл. 4. В формуле (2) значение бюджета также исключено намеренно, чтобы был ясен замысел исследования и огромные суммы не мешали бы анализу, гораздо важнее значение соотношения.

Графические результаты расчета по формуле (2) для всего диапазона значений переменных показаны на рис. 2.

Очевидна нелинейная зависимость оценки уровня защиты ПДн (R_{GDPR}) от степени зрелости существующей базовой системы ИБ предприятия (L_{ITSM}) в области значительных соотношений бюджета, выделяемого на обеспечение ИБ и суммы потенциального штрафа. Например, начиная от N_{GDPR} = 0,01 (кратности бюджета 100) и менее, как показывают расчеты, невозможно получить оценку уровня защиты ПДн (R_{GDPR}) выше 1%, даже при максимальных показателях степени зрелости базовой системы ИБ (L_{ITSM} = 1). Начиная с N_{GDPR} = 0,1 (кратности бюджета 10) и более можно говорить о кусочно-линейной зависимости уровня R_{GDPR}, но также в слабой связи с показателями L_{ITSM}, т.к. максимальное значение R_{GDPR} составит только 10%.

Начиная от N_{GDPR} = 0,001 (кратности бюджета 1000), как показывают расчеты, оценку уровня защиты ПДн (R_{GDPR}) становится неотличимой от нуля при любом показателе степени зрелости базовой системы ИБ (L_{ITSM}). Соответственно, эту границу можно определить как «границу катастрофы», поскольку предприятие не сможет гарантированно парировать ни один риск штрафов за несоответствия известным установленным требованиям GDPR. Этот же показатель можно применять при анализе качества решений, предлагаемых консультантами, в частности, какие оценки рисков они готовы представить для гарантированного уровня защиты ПДн и, при определённых условиях, и обшей системы обеспечения ИБ для предприятия.

Таблица 4

Расчета зрелости системы защиты ПДн

N_{GDPR}	Log10 (N_{GDPR})	Оценка уровня защиты ПДн, RGDPR				
		Степень зрелости L_{ITSM} = 0	Степень зрелости L_{ITSM} = 0,25	Степень зрелости L_{ITSM} = 0,5	Степень зрелости L_{ITSM} = 0,75	Степень зрелости L_{ITSM} = 1
1	0,000	0	0,25	0,5	0,75	1
0,5	-0,301	0,00000	0,12500	0,25000	0,37500	0,50000
0,1	-1,000	0,00000	0,02500	0,05000	0,07500	0,10000
0,05	-1,301	0,00000	0,01250	0,02500	0,03750	0,05000
0,01	-2,000	0,00000	0,00250	0,00500	0,00750	0,01000
0,005	-2,301	0,00000	0,00125	0,00250	0,00375	0,00500
0,001	-3,000	0,00000	0,00025	0,00050	0,00075	0,00100
0,0005	-3,301	0,00000	0,00013	0,00025	0,00038	0,00050
0,0001	-4,000	0,00000	0,00003	0,00005	0,00008	0,00010
0,00005	-4,301	0,00000	0,00001	0,00003	0,00004	0,00005
0,00001	-5,000	0,00000	0,00000	0,00001	0,00001	0,00001

DOI: 10.21681/2311-3456-2020-04-66-75

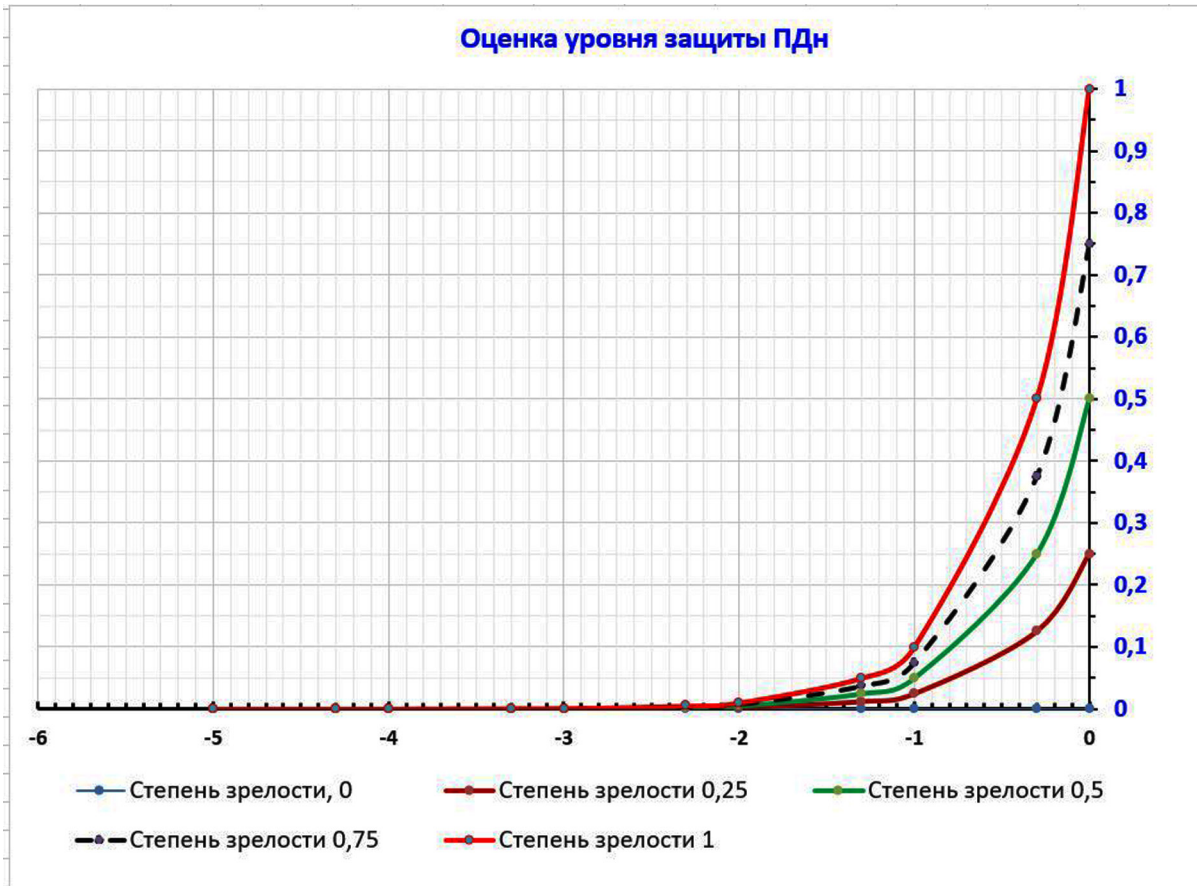

Рис. 2. Результаты расчета уровня защиты ПДн по Табл. 4

Важность учета затрат на обеспечение безопасности ПДн

В качестве дополнения исследования рассмотрим международные оценки важности учета затрат для обеспечения безопасности критических данных (в том числе ПДн). В актуальном отчете «Data Protection Report» Veeam Software[2] представлены результаты исследования ключевых бизнес-процессов и данных, которые необходимо защищать. Для целей данной публикации отметим ключевой результат – грань ценности между критичными и обычными сервисами стирается: например, ориентировочная стоимость часа простоя для приоритетного и обычного приложения составляет 67.651 и 61.642 долларов США соответственно. Кроме того, показано, что более 95% компаний по всему миру сталкивались с неожиданными сбоями, и в среднем сбой продолжался 117 минут, соответственно, можно определить средний ущерб только от одного неожиданного сбоя в сумме 125.972 долларов США. Международные компании в среднем тратят на технологии защиты данных 484.591 долларов США в год. Отметим, что данная сумма примерно в 400 раз меньше штрафа, наложенного на авиакомпанию British Airways (пример рассмотрен выше). В продолжении анализа экономических аспектов можно заметить, что 48% компаний в мире считают, что цифровая трансформация поможет им сократить издержки. Для предприятий в Российской Федерации очень важная проблема – это экономическая неопределенность (29%), соответствие нормативным требованиям (26%) и недостаток знаний для внедрения необходимых технологий (26%). Следует отметить, что 30% респондентов назвали отсутствие бюджетов главной проблемой в области защиты данных.

В докладе Данилова[3] «Технологии обнаружения компьютерных атак» (компания Infotecs), показано, что за 1-е полугодие 2019 г. SOC обрабатывал 433.083.046 событий ИБ, из них выявлено 573 инцидентов ИБ, и за 1-е полугодие 2018, соответственно, обработано 149.009.215 событий ИБ и выявлено 177 инцидентов ИБ. Легко видеть, что доля инцидентов к общему числу событий ИБ примерно одна миллионная, что ставит серьезный вопрос об экономическом обосновании целесообразности внедрения средств защиты, доказанная результативность которых явно не окупается с учетом более чем существенных затрат.

Можно отметить обзор (май 2020 г.) экспертов Palo-Alto[4], в котором отмечаются реалии современного менеджмента при принятии решения о «смещении» границы безопасности. В частности, философия Zero Trust

2 https://www.cnews.ru/news/line/2020-06-02_veeam_predstavila_issledovanie

3 https://soc-forum.ib-bank.ru/files/files/SOC2019/14%20Danilov.pdf

4 https://blog.paloaltonetworks.com/2020/05/network-cloud-native-applications/

требует «смещения» границ доверия как можно ближе к уровню приложений, но существующие методы управления, сложности организационного порядка постоянно отодвигают ее. В результате лица, принимающие решения, вынуждены формировать управленческие решения фактически только исходя из бюджета на ИБ.

Заключение

В представленной публикации рассмотрены некоторые вопросы определения экономически оптимальных областей для принятия взвешенных решений о привлечении консультантов при оценке соответствия требованиям General Data Protection Regulation (GDPR). С учетом сложившейся практики выполнения проектов по обеспечению защиты ПДн в Российской Федерации для предприятий по-прежнему остается актуальной проблемой принятие мотивированного решения о создании экономически эффективной и адекватной системы защиты ПДн. Несмотря на наличие в Российской Федерации Федерального закона № 152-ФЗ «О защите персональных данных» для многих предприятий положения GDPR являются новыми и могут оказывать серьезное негативное воздействие в силу рисков значительных финансовых санкций.

Предложены рекомендации для оценки уровня зрелости существующей системы ИБ, оценки рисков прерывания нормальной деятельности, определения необходимости совершенствования системы защиты ПДн требованиям GDPR. Полученные результаты могут применяться для экономического обоснования технических решений при оценке соответствия различным законодательным требованиям, что позволит снизить риски международной деятельности предприятий.

Литература

1. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. (дата обращения 22.06.2020)
2. GDPR Fines Tracker & Statistics [Электронный ресурс]. URL: https://www.privacyaffairs.com/gdpr-fines. (дата обращения 22.06.2020)
3. Statistics: Highest individual fines (Top 10) [Электронный ресурс]. URL: https://www.enforcementtracker.com/?insights. (дата обращения 22.06.2020)
4. A Very Brief Introduction to the GDPR Recitals [Электронный ресурс]. – 2019. - URL: https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2019/a-very-brief-introduction-to-the-gdpr-recitals. (дата обращения 22.06.2020)
5. Adequacy decisions [Электронный ресурс]. URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. (дата обращения 22.06.2020)
6. About EDPB [Электронный ресурс]. URL: https://edpb.europa.eu/about-edpb/about-edpb_en (дата обращения 22.06.2020)
7. Власов Р.Б. Применения общего регламента Европейского Союза по защите персональных данных к российским компаниям: Проблемы и способы их решения // Бизнес. Образование. Право. – 2019. – № 1 (46). – С. 383-388.
8. Mannhardt F., Petersen S.A., Oliveira M.F. Privacy challenges for process mining in human-centered industrial environments. В сборнике: Proceedings - 2018 International Conference on Intelligent Environments, IE 2018 14. 2018. С. 64-71.
9. Анализ возможных последствий и влияния регламента General Data Protection Regulation (GDPR) Европейского Союза на бизнес российских операторов персональных данных (телекоммуникационные компании, интернет компании) предоставляющих услуги через интернет для лиц в странах ЕС в контексте действующего и вступающего в силу регулирования в Российской Федерации. – М. Институт исследований интернета, 2017. – 196 с.
10. Лившиц И. Учет активов при планировании и проведении аудитов в системе менеджмента информационной безопасности на соответствие требованиям ISO/IEC 27001:2013 // Управление качеством. – 2014. – № 11. – С. 36-39
11. Лившиц И.И. Подходы к оценке систем менеджмента информационной безопасности на соответствие требованиям ISO / IEC 27001:2013 // Управление качеством. – 2014. – № 6. – С. 41-46.
12. Лившиц И.И. Стоматологический программный комплекс MasterClinic. Принципы успешного внедрения и сопровождения / Агаджанян Э.Г., Лапин А.В., Лившиц И.И. // Врач и информационные технологии. – 2007. – № 2. – С. 50-58.
13. Besik S.I., Freytag J.-C. A formal approach to build privacy awareness into clinical workflows. Software-Intensive Cyber-Physical Systems. 2019.
14. Pikulík T., Štarchoň P. GDPR compliant methods of data protection. В сборнике: 6th SWS International Scientific Conferences on social sciences 2019 Conference proceedings. – 2019. – С. 561-572.
15. Laune D., Arnavielhe S., Bousquet J., Viart F., Bedbrook A., Mercier J., Lun San Luk G., deVries G., Spreux O. Adaptation of the general data protection regulation (GDPR). Revue des Maladies Respiratoires. – 2019. – Т. 36. – № 9. – С. 1019-1031.
16. Lysakova L. Social media privacy: Myth or reality? В сборнике: 76-я научная конференция студентов и аспирантов Белорусского государственного университета Материалы конференции. В 3-х частях. Редколлегия: В.Г. Сафонов [и др.]. 2019. С. 595-598.
17. Brodin, M. A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. Eur J Secur Res. – 2019. – 4, P. 243–264 doi: 10.1007/s41125-019-00042-z
18. Framework for Demonstrable GDPR Compliance [Электронный ресурс]. URL: https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Toolkit/Accountability_Roadmap_for_Demonstrable_GDPR_Compliance.pdf (дата обращения 22.06.2020)
19. Martin N., Matt C., Niebel C. et al. How Data Protection Regulation Affects Startup Innovation. Inf Syst Front 21, P. 1307–1324. – 2019. – doi:10.1007/s10796-019-09974-2.

20. Денисов И.С., Ахматова Д.Р., Кабакова В.М. Сравнительная характеристика GDPR и Российского законодательства о персональных данных // Экономика. Право. Общество. – 2019. – № 1 (17). – С. 21-27.
21. Гришина Н.Ю., Болдырева Е.Л., Дуйсембина Е.О. Влияние интернет-технологий на процесс принятия решений как новый политический тренд (на примере компании «Кембридж Аналитика»). Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Гуманитарные и общественные науки. – 2019. – Т. 10. – № 1. – С. 69-80.
22. Lăzăroiu G., Kovacova M., Kliestikova J., Kubala P., Valaskova K., Dengov V.V. Data governance and automated individual decision-making in the digital privacy general data protection regulation. Administratie si Management Public. – 2018. – Т. 2018. – № 31. – С. 132-142.
23. Jurkevich T., Sedjakins O. International transfers of personal data. В сборнике: 6th SWS International Scientific Conferences on social sciences 2019 Conference proceedings. 2019. С. 119-126.
24. Agbozo E., Alhassan D., Spassov K. Personal data and privacy barriers to e-Government adoption, implementation and development. Communications in Computer and Information Science. 2019. Т. 947. С. 82-91.
25. Лившиц И.И. Проектирование, создание и внедрение комплексных систем информационной безопасности на базе ISO / IEC 27001:2005 // Электросвязь. – 2010. – № 4. – С. 49-51.
26. Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами: автореферат дис. ... доктора Технических наук: 05.13.19 / Лившиц Илья Иосифович; [Место защиты: ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук], 2018.

Рецензент: *Молдовян Александр Андреевич, начальник научно-исследовательского отдела проблем информационной безопасности, доктор технических наук, профессор, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, Россия. E-mail: maal305@yandex.ru*

ASSESSMENT OF THE IMPACT OF GENERAL DATA PROTECTION REGULATION ON ENTERPRISE SECURITY IN THE RUSSIAN FEDERATION

Livshitz I. [5]

Abstract

The purpose of the study *is to analyze the existing requirements for personal data security and assess the impact of these requirements on the enterprises security in the Russian Federation.*

Research method: *the problem of ensuring the security of personal data in accordance with the requirements of the Federal law of the Russian Federation FZ-152 and the international General Data Protection Regulation is investigated. The article analyzes the possible risks of interrupting the normal activities of enterprises in the Russian Federation due to violations of these requirements for personal data protection and the imposition of significant fines by international regulators. Numerical relationships are estimated between the amount of fines for violations of established requirements, including General Data Protection Regulation, and the cost of creating an effectiveness personal data protection system. Estimates of the permissible degree of influence of the General Data Protection Regulation requirements on the enterprises security in the Russian Federation are obtained.*

Research result: *a study and comparison of possible penalties for violation of compliance with the requirements of the Federal law of the Russian Federation FZ-152 and the international General Data Protection Regulation was performed. Risk assessments of sanctions for violation of the established requirements for personal data protection were obtained. The analysis of the cost of preparing a personal data protection system for compliance with the requirements of the General Data Protection Regulation was performed. Based on the data obtained, examples of calculating the degree of maturity of the security system are presented – based on the ratio of the share of the budget allocated for security in relation to the cost of creating an effectiveness personal data protection system and based on the ratio of the amount of the fine for violation of the established requirements. The importance of accounting for the costs of personal data security to ensure the security of enterprises in the Russian Federation, taking into account the requirements of the General Data Protection Regulation, is shown.*

5 Ilya Livshitz, Dr.Sc., Associate Professor, Professor of Information Technology Security at ITMO University, St. Petersburg, Russia. E-mail: Livshitz.il@yandex.ru

Keywords: *personal data, risk assessment, budget, damage, Federal law, threat, level of maturity, system, conformity assessment.*

References

1. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. (access date 22.06.2020)
2. GDPR Fines Tracker & Statistics [Электронный ресурс]. URL: https://www.privacyaffairs.com/gdpr-fines. (access date 22.06.2020)
3. Statistics: Highest individual fines (Top 10). URL: https://www.enforcementtracker.com/?insights. (access date 22.06.2020)
4. A Very Brief Introduction to the GDPR Recitals. 2019. URL: https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2019/a-very-brief-introduction-to-the-gdpr-recitals. (access date 22.06.2020)
5. Adequacy decisions. URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. (access date 22.06.2020)
6. About EDPB. URL: https://edpb.europa.eu/about-edpb/about-edpb_en (access date 22.06.2020)
7. Vlasov R. B. Application of the General regulation of the European Union on personal data protection to Russian companies: Problems and solutions // Business. Education. Right. 2019. № 1 (46). Pp. 383-388.
8. Mannhardt F., Petersen S.A., Oliveira M.F. Privacy challenges for process mining in human-centered industrial environments. Proceedings - 2018 International Conference on Intelligent Environments, IE 2018 14. 2018. Pp. 64-71.
9. Analysis of the possible consequences and impact of the General Data Protection Regulation (GDPR) of the European Union on the business of Russian personal data operators (telecommunications companies, Internet companies) providing services via the Internet for individuals in the EU countries in the context of current and effective regulation in the Russian Federation. - M. Institute for Internet research, 2017. 196 p.
10. Livshits I. Asset accounting when planning and conducting audits in the information security management system for compliance with the requirements of ISO/IEC 27001: 2013 // Quality management, 2014, N11, Pp. 36-39
11. Livshits I. Approaches to the assessment of information security management systems for compliance with the requirements of ISO / IEC 27001: 2013 // Quality management, 2014, N6, Pp. 41-46.
12. Livshits I. Dental software package MasterClinic. Principles of successful implementation and support / Agajanyan E. G., Lapin A.V., Livshits I. I. / / Doctor and information technologies.2007. N. 2. Pp. 50-58.
13. Besik S.I., Freytag J.-C. A formal approach to build privacy awareness into clinical workflows. Software-Intensive Cyber-Physical Systems. 2019.
14. Pikulík T., Štarchoň P. GDPR compliant methods of data protection. 6th SWS International Scientific Conferences on social sciences 2019 Conference proceedings. 2019. Pp. 561-572.
15. Laune D., Arnavielhe S., Bousquet J., Viart F., Bedbrook A., Mercier J., Lun San Luk G., deVries G., Spreux O. Adaptation of the general data protection regulation (GDPR). Revue des Maladies Respiratoires. 2019. Vol. 36. N 9. Pp. 1019-1031.
16. Lysakova L. Social media privacy: Myth or reality? 76th scientific conference of students and postgraduates of the Belarusian state University conference Materials. In 3 parts. Editorial Board: V. G. Safonov [et al.]. 2019. Pp. 595-598
17. Brodin, M. A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. Eur J Secur Res. – 2019. – 4, Pp. 243–264 doi: 10.1007/s41125-019-00042-z
18. Framework for Demonstrable GDPR Compliance. URL: https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Toolkit/Accountability_Roadmap_for_Demonstrable_GDPR_Compliance.pdf (access date 22.06.2020)
19. Martin N., Matt C., Niebel C. et al. How Data Protection Regulation Affects Startup Innovation. Inf Syst Front 21, P. 1307–1324. – 2019. – doi:10.1007/s10796-019-09974-2.
20. Denisov I. S., Akhmatova D. R., Kabakova V. M. Comparative characteristics of GDPR and Russian legislation on personal data // Economy. Right. Society. 2019. № 1 (17). Pp. 21-27.
21. Grishina N. Yu., Boldyreva E. L., Duisembina E. O. Influence of Internet technologies on the decision-making process as a new political trend (on the example of Cambridge Analytica). Scientific and technical Bulletin of the Saint Petersburg state Polytechnic University. Humanities and social Sciences, 2019, Vol. 10, No. 1, Pp. 69-80.
22. Lăzăroiu G., Kovacova M., Kliestikova J., Kubala P., Valaskova K., Dengov V.V. Data governance and automated individual decision-making in the digital privacy general data protection regulation. Administratie si Management Public. 2018. Vol. 2018. № 31. Pp. 132-142.
23. Jurkevich T., Sedjakins O. International transfers of personal data. 6th SWS International Scientific Conferences on social sciences 2019 Conference proceedings. 2019. Pp. 119-126.
24. Agbozo E., Alhassan D., Spassov K. Personal data and privacy barriers to e-Government adoption, implementation and development. Communications in Computer and Information Science. 2019. Vol. 947. Pp. 82-91.
25. Livshits I. Design, creation and implementation of integrated information security systems based on ISO / IEC 27001: 2005 // Telecommunications, 2010, No. 4, Pp. 49-51.
26. Livshits I. Models and methods of audit of information security of integrated control systems for complex industrial objects: abstract of dis. ... doctor of Technical Sciences: 05.13.19 / Livshits Ilya Iosifovich; [Place of protection: Saint Petersburg Institute of Informatics and automation of the Russian Academy of Sciences], 2018.