Правоприменение открытых данных с учетом требований по информационной безопасности

Марков А. С.[1]

Ключевые слова: *общедоступная информация, открытые государственные данные, открытое правительство, Цифровая Россия, открытые технологии, информационные системы общего пользования, целостность, доступность, конфиденциальность, безопасность информации, безопасность веб-приложений.*

Аннотация. *В работе рассмотрен вопрос наличия противоречия между требованиями по защите информации и требованиями по открытости государственных данных. Приведена классификация открытых и общедоступных государственных данных. Указаны общедоступные источники данных, которые можно использовать при менеджменте информационной безопасности. Показана полнота и достаточность мер по защите открытых ресурсов в информационных системах общего пользования в России. Сделан вывод о достаточности и полноте таксономий в области безопасности веб-ресурсов. Приведен сравнительный анализ отдельных интернет-порталов по открытым данным. Отмечены проблемные вопросы использования открытых данных в области информационной безопасности и указаны некоторые направления их решения.*

DOI: 10.21681/2412-8163-2017-3-86-96

Введение

Развитие парадигм электронного и открытого правительств обусловило внимание к так называемым открытым государственным данным (англ. “open government data”, далее – ОД) [1–3], которые должны представляться интернет-порталами различных систем государственных органов в общий доступ для дальнейшей обработки в различных информационных системах[2]. В связи с указанным следует отметить два фактора информатизации общества:

- одним из путей совершенствования государственного управления является внедрение некоторых принципов его открытости, включая размещение и сопровождение ОД, часть из которых обеспечивает контур обратной связи общественного контроля;
- продолжается развитие «открытых» технологических движений, начиная от использования программных продуктов с открытым кодом (open source) и заканчивая открытыми концепциями оценки соответствия (Common Criteria), целью которых является повышение эффективности исследований и производств ИТ-продуктов и систем.

Что касается обработки ОД, то можно указать следующее:

- в стране продолжается формирование нормативно-правовых требований по целостности и доступности информационных ресурсов общего пользования и общего доступа;
- противостояние угрозам в отказе в обслуживании (доступности ресурсов) в киберпространстве представляется наиболее сложной задачей обеспечения безопасного функционирования интернет-порталов.

Указанное обусловливает научный интерес к понятию именно информационной безопасности

[2] Постановление Правительства РФ от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных».

[1] ***Марков Алексей Сергеевич,*** доктор технических наук, сертифицированный специалист по информационной безопасности (CISSP), член Экспертного Совета при Правительстве Российской Федерации, Российская Федерация, г. Москва.
E-mail: a.markov@bmstu.ru

ОД. Отметим, что в бытовом плане, с точки зрения устаревшего взгляда на обеспечение *безопасности информации* (как обеспечение секретности и конфиденциальности информации), процедура защиты открытых данных как бы вступает в кажущееся противоречие с самими понятиями открытости и общедоступности. Однако, это, конечно, не так, если рассматривать понятие *информационной безопасности в* общепринятом международном понимании (information security), когда все открытые ресурсы информационных систем могут иметь широкий спектр угроз в информационной сфере, в первую очередь это касается угроз целостности и доступности.

Исследованию состояния вопроса обеспечения информационной безопасности ОД и посвящена данная статья.

Понятие открытых данных и классификации

К открытым государственным данным, как правило, относят общедоступные данные в электронном формате, официально предоставляемые государственными органами для дальнейшего свободного использования. Например, на сервере органов государственной власти РФ указанные данные представляются как «*информация о деятельности государственных органов и органов местного самоуправления, размещенная в сети Интернет в формате, обеспечивающем ее автоматическую обработку в целях повторного использования без предварительного изменения человеком (машиночитаемый формат), и может свободно использоваться в любых соответствующих закону целях любыми лицами независимо от формы ее размещения*[3].

Выделяют базовые *принципы* ОД, такие как: первичность, полнота, актуальность, пригодность к машинной обработке, отсутствие дискриминации по доступу, отсутствие проприетарных форматов[4], лицензионная чистота и другие [3].

В техническом плане наборы ОД обладают свойством *интероперабельности*, так как должны отсутствовать ограничения по доступу и реализации данных, а их форматы и интерфейсы должны иметь открытый вид.

Согласно методическим рекомендациям ФАНО России[5], классификация типов открытых данных представляется по следующим основным критериям: предметная область, формат данных, структура данных (линейная, иерархическая и т.д.), объем данных, способ публикации, способ хранения, периодичность обновления, актуальность данных.

На рис. 1 показаны наборы ОД, представленные на интернет-портале открытых данных РФ[6].

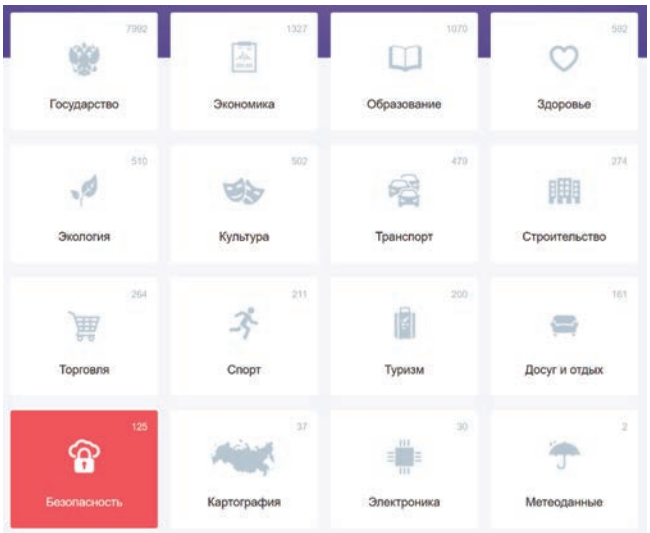

Рис. 1. Наборы открытых государственных данных России

Как отмечалось, понятие ОД определено отнесением наборов данных к государственному ресурсу при условиях размещения их в общее пользование в сети Интернет в заданных форматах (рис. 2). Таким образом, ОД являются подмножеством *общедоступных государственных данных (ОДД)*, характеризуемых дополнительными наложенными ограничениями, главным образом, в интерфейсах и формате представления на интернет-портале:

$$\text{ОД} \underset{def}{\subseteq} \text{ОДД}.$$

При этом нет технических препятствий как для перевода общедоступных данных в формат открытых данных, так и дальнейшего преобразования ОД [4].

Легко заметить (рис.2), что в законодательном плане выделяются две категории *общедоступных* данных, к которым государство предъявляет требования по информационной безопасности (ИБ):

- общедоступные персональные данные[7] в информационных системах обработки персональных данных (ИСПДн);

[3] http://ar.gov.ru/inform_otkritost_05_otkritii_dannie/index.html

[4] http://data.gov.ru/file-converting-service

[5] http://fano.gov.ru/common/upload/3.0.pdf

[6] http://data.gov.ru/, дата обращения: 01.10.2017.

[7] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Рис. 2. Классификация информации по доступности

› общедоступные данные в информационных системах общего пользования (ИСОП), что собственно и есть ОД (см. ниже).

В целевом плане можно выделить два подкласса наборов общедоступных данных в области информационной безопасности:

1. Наборы ОД, касающиеся официальной деятельности органов государственной власти[8];

2. Иные наборы общедоступных государственных данных, которые можно использовать в системах менеджмента ИБ.

Что касается органов государственной власти, то в РФ (согласно Постановлению Правительства РФ от 15.04.1995 № 333 и Постановлению Правительства РФ от 26.06.1995 № 608) существуют три регулятора в области ИБ: Минобороны России, ФСБ России, ФСТЭК России, действующие в рамках своих компетенций. Наиболее полезную и полную информацию, касающиюся вопросов ИБ, можно получить на официальном интернет-портале ФСТЭК России – www.fstec.ru, пройдя в раздел «Открытые данные» (табл. 1).

Таблица 1. Наборы открытых данных ФСТЭК России

№	Название набора данных	Форматы
	Государственный реестр сертифицированных средств защиты информации	ods, csv
	Перечень испытательных лабораторий	ods, csv
	Перечень органов по аттестации	ods, csv
	Перечень органов по сертификации	ods, csv
	Перечень подведомственных организаций	Csv
	Перечень территориальных органов	Csv
	План проведения плановых проверок по вопросам лицензионного контроля	ods, csv
	План проведения плановых проверок по вопросам экспортного контроля	ods, csv
	Реестр лицензий СЗКИ	ods, csv
	Реестр лицензий ТЗКИ	ods, csv

[8] Распоряжение Правительства РФ от 10.07.2013 № 1187-р «О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных».

Разумеется, на портале ФСТЭК России можно найти другие общедоступные данные в области ИБ, как-то: реестр экспертных организаций, реестр образовательных учреждений и центров, нормативно-правовые акты, методические документы, адресная, антикоррупционная, конкурсная информация и др. Особое внимание следует уделить, безусловно, Банку данных угроз безопасности информации[9].

Иные наборы общедоступных данных легко получить методами конкурентной разведки [5] из общедоступных государственных источников (табл. 2).

На рис. 3 приведен пример, когда поисковик использует общедоступные данные по юридическим лицам, в данном случае, декларирующих лицензионный вид деятельности – техническую защиту информации. Другим примером является услуга портала Минкомсвязи России по поиску на карте ближайшего удостоверяющего центра[10].

Таблица 2. Примеры общедоступных государственных источников

Наборы данных, документы	Источники
Методическое обеспечение деятельности	
Стандарты, методические документы по ИБ	http://www.gost.ru/ https://www.tc26.ru/ http://www.cbr.ru/credit/gubzi_docs/
Диссертации, рецензируемые публикации, патенты, свидетельства	http://vak.ed.gov.ru/dis-list https://elibrary.ru http://www1.fips.ru/wps/wcm/connect/content_ru/ru/inform_resources/inform_retrieval_system/
Рекомендации	http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert
Услуги, поставки	
Реестр удостоверяющих центров	http://minsvyaz.ru/ru/activity/ govservices/certification_authority/
Единый реестр российских программ	https://reestr.minsvyaz.ru/
Проверка соисполнителя работ	
Реестр недобросовестных поставщиков	http://fas.gov.ru/ http://zakupki.gov.ru/epz
Сведения о гос. регистрации юр. лиц	https://egrul.nalog.ru/
Единый фед. реестр сведений о банкротстве	https://bankrot.fedresurs.ru/
Единый реестр субъектов МСП	https://rmsp.nalog.ru/
БД исполнительных производств	http://fssprus.ru/iss/ip/
Проверка персонала	
ПДн госслужащих	Порталы госорганов
Судебные дела	Порталы судов, например: http://mos-gorsud.ru
АС «Российский Паспорт»	http://services.fms.gov.ru/info-service.htm?sid=2000
Фед.реестр сведений о документах об образовании	http://frdocheck.obrnadzor.gov.ru/
БД исполнительных производств	http://fssprus.ru/iss/ip/
ГАС РФ «Правосудие»	https://bsr.sudrf.ru
Планирование инвестиций в регионы	
Бюджет субъекта РФ	http://budget.gov.ru https://minfin.ru/opendata/
Различная обобщенная статистика	http://www.gks.ru

[9] http://bdu.fstec.ru/threat

[10] http://minsvyaz.ru/ru/activity/govservices/2/

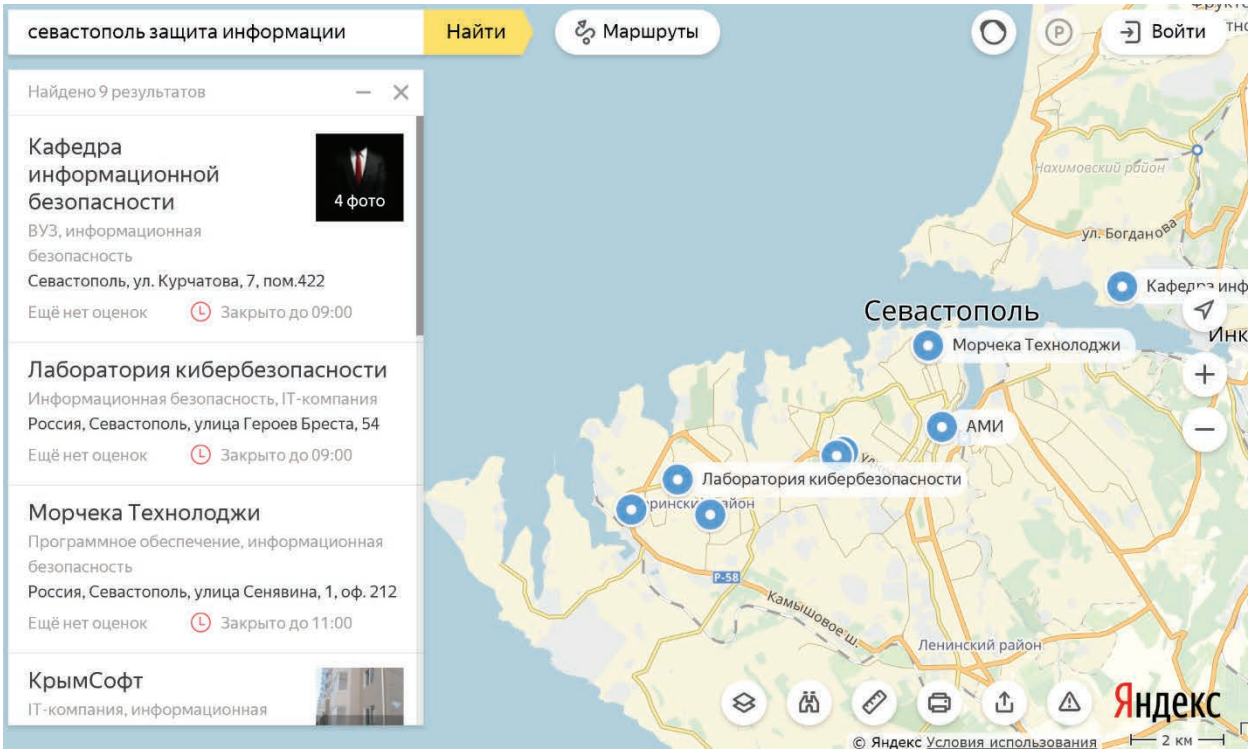

Рис. 3. Пример геометок на карте по запросу в поисковике

Следует констатировать, что использование ОД и открытых данных негосударственных корпораций и ассоциаций дает мощный синергетический эффект [5].

Угрозы открытых данных в информационной среде

Информационную безопасность открытых государственных данных можно определить как свойство защищенности ОД от угроз в информационной сфере. Можно разделить указанные угрозы на возможные нарушения технических требований к ОД и злоупотребления их использования (data abuse [6]). В правовом поле обычно выделяют три актуальных направления угроз ОД:

1. Угрозы безопасности информации, связанные с жизненным циклом ОД и организационно-техническими системами обеспечения ОД;

2. Угрозы, касающиеся защиты личной и семейной тайн или тайны частной жизни (персональных данных);

3. Угрозы, связанные с национальной (государственной) безопасностью.

Наиболее дискуссионными, конечно, считаются угрозы, связанные с национальной безопасностью. Как известно, открытые ресурсы являются основным источником современной разведки, независимо, относится она к бизнес-разведке или имеет национальный статус. Достаточно хорошо известны факты использования потенциала открытых данных в криминальных целях[11]. ОД, кроме всего прочего, позволяют роботизировать процесс сбора и когнитивного анализа разведанных. Эти моменты описаны в профессиональной литературе и даже стандартах[12] [7].

Угрозы, касающиеся приватных тайн, относят к вопросу защиты *прав субъектов* персональных данных, что сейчас достаточно проработано [8]. Пересечение интересов может происходить при раскрытии, скажем, доходов госслужащих в антикорупционных целях.

Что касается угроз безопасности информации, то можно выделить:

- угрозы целостности и доступности собственно ОД;
- угрозы целостности, доступности и конфиденциальности ресурсов систем обеспечения (например, информационного, программного, технического обеспечения и др.) ИСОП.

К примеру, если мы представим, что на веб-сайте зафиксированы просто документы в формате ОД, то налицо угрозы их целостности и доступности. Если веб-портал имеет функции регистрации пользователей и поддержки переписки, уже возникают задачи защиты указанной информации

[11] http://www.interfax.ru/russia/452799

[12] https://www.ise.gov/sites/default/files/2012infosharingstrategy.pdf

дополнительно от угроз нарушения конфиденциальности. Аналогичные задачи возникают для защиты внутренней структуры портала, когда уже имеется разграничение доступа к ресурсам с момента разграничения привилегий администратора и пользователей. Современные ИСОП подключены к системе межведомственного электронного взаимодействия (СМЭВ) и поддерживают Единую систему идентификации и аутентификации (ЕСИА), а некоторые еще и включают в себя платежные компоненты. Надо понимать, что современные ОД могут иметь распределенный вид (например, link open data [9]) – это накладывает требования обеспечения не только физической, но и логической (семантической) целостности открытых ресурсов и др.

Далее рассмотрим нормативные требования к подобным системам.

Нормативные требования по информационной безопасности

Можно утверждать, что в России сформирована нормативная база как к объектам информатизации (автоматизированным системам), обрабатывающим ОД, так и к средствам защиты ОД [10, с. 47].

Требования по безопасности информации в информационных системах, обрабатывающих ОД, определены Постановлением Правительства РФ от 18 мая 2009 г. № 424 и конкретизированы совместным Приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. Согласно указанному приказу введены два класса информационных систем общего пользования (ИСОП). Функционирование ИСОП 1-го класса (ИСОП-1) ориентировано на высшие органы государственной власти (точнее, нарушения работы таких ИСОП могут повлечь угрозу безопасности РФ), поэтому такая система находится в компетенции ФСБ России. Статус ИСОП-1 определяется Решением руководителя федерального органа исполнительной власти.

Что касается всех остальных ИСОП (то есть ИСОП-2), то при их построении можно использовать нормативно-правовые акты (НПА) ФСТЭК России, которые в данном случае сами относятся к общедоступным данным (что не скажешь о документах других регуляторов ИБ, зачастую игнорирующих следствия принципа Керкгоффса [10, с.27]). Для введения в эксплуатацию ИСОП-2 достаточно уведомления ФСТЭК России.

Требования по составу сертифицированных средств защиты информации ИСОП представлены в табл. 3.

Что касается требований к средствам защиты информации (за исключением криптографических), то ФСТЭК России в настоящее время формирует их на основании так же *открытой* методологии Common Criteria [11]. В настоящее время в ИСОП-2 применяются средства защиты информации *4-го класса защищенности*, что соответствует 3-му усиленному оценочному уровню доверия – *ОУД3+* [10, с. 68] (табл. 4).

Таблица 3. Перечень средств защиты информации, подлежащих сертификации

Классы средств защиты информации	Вид сертификата соответствия	
	ИСОП-1	**ИСОП-2**
СКЗИ (ЭЦП)	ФСБ	ФСБ
Антивирусные средства	ФСБ	ФСБ или ФСТЭК
Межсетевые экраны	ФСБ	ФСБ или ФСТЭК
Системы обнаружения компьютерных атак	ФСБ	ФСБ или ФСТЭК
Средства контроля доступа	ФСБ	ФСБ или ФСТЭК

Таблица 4. Перечень специальных нормативных документов по средствам защиты информации

Средства защиты информации	**Методические документы (профили защиты)**
Антивирусные средства	ИТ.САВЗ.А4.ПЗ; ИТ.САВЗ.Б4.ПЗ; ИТ.САВЗ.В4.ПЗ; ИТ.САВЗ.Г4.ПЗ
Межсетевые экраны	ИТ.МЭ.А4.ПЗ; ИТ.МЭ.Б4.ПЗ; ИТ.МЭ.В4.ПЗ; ИТ.МЭ.Г4.ПЗ; ИТ.МЭ.Д4.ПЗ
Системы обнаружения компьютерных атак	ИТ.СОВ.С4.ПЗ; ИТ.СОВ.У4.ПЗ
Средства контроля доступа	РД СВТ (класс защиты – СВТ-5)[1]
Операционные системы со встроенными средствами контроля доступа	ИТ.ОС.А4.ПЗ; ИТ.ОС.Б4.ПЗ; ИТ.ОС.В4.ПЗ

[1] В текущем году ожидается замена Руководящего документа по средствам вычислительной техники (Гостехкомиссия, 1992 г.) на современные профили защиты.

Надо понимать, что ФСТЭК России *дополнительно* определяет требования (в части некриптографических методов) к государственным информационным системам (ГИС) и информационным системам обработки персональных данных (ИСПДн) соответственно приказами 2013 г. №№ 17 и 21. (табл. 5.). Данные приказы придерживаются квази риск-ориентированного подхода, то есть допускают обоснованное снижение числа мер защиты в зависимости от ограниченности ИТ-архитектуры системы.

Таблица 5.Организационные и технические меры защиты информации в информационных системах

№	Группы организационно-технических мер		ИС	
	Префикс	Название меры	ГИС	ИСПДн
1	ИАФ	Идентификация и аутентификация субъектов доступа и объектов доступа	+	+
2	УПД	Управление доступом субъектов доступа к объектам доступа	+	+
3	ОПС	Ограничение программной среды	+	+
4	ЗНИ	Защита машинных носителей информации	+	+
5	РСБ	Регистрация событий безопасности	+	+
6	АВЗ	Антивирусная защита	+	+
7	СОВ	Обнаружение вторжений	+	+
8	АНЗ	Контроль (анализ) защищенности информации	+	+
9	ОЦЛ	Обеспечение целостности информационной системы и информации	+	+
10	ОТД	Обеспечение доступности информации	+	+
11	ЗСВ	Защита среды виртуализации	+	+
12	ЗТС	Защита технических средств	+	+
13	ЗИС	Защита информационной системы, ее средств, систем связи и передачи данных	+	+
14	ИНЦ	Выявление инцидентов и реагирование на них	-	+
15	УКФ	Управление конфигурацией автоматизированной системы управления и ее системы защиты	-	+

В настоящее время при проектировании и аттестации защищенных систем, а также сертификации средств защиты информации, обязательной процедурой является проверка уязвимостей. Поэтому для полноты картины кратко рассмотрим вопрос возможности контроля защищенности веб-порталов как базовой платформы организации ИСОП.

Уязвимости и атаки на ресурсы веб-порталов

Веб-порталы в настоящее время наиболее часто подвергаются компьютерным атакам со стороны разного рода нарушителей. Так, по оценкам компании WhiteHat Security, процент компьютерных атак на веб-ресурсы составляет 40 % от всех зарегистрированных в течение прошлого года атак[13].

Пример типового защищенного веб-портала представлен на рис. 4. На рисунке видно и основные компоненты веб-портала (веб-сервер, сервер пользовательских приложений, систему управления базой данных, включая ОД), и типовые средства защиты информации. Несмотря на средства защиты (по известной причине крайней сложности и динамичности программных подсистем), веб-портал нуждается в постоянной проверке на наличие уязвимостей и проверке угроз их реализации (возможности проведения компьютерных атак).

Однако, по аналогии с российской нормативной базой (см. выше), можно констатировать, что в мире сформировалось понимание безопасности веб-портала и имеются соответствующие реестры и стандарты описания уязвимостей, угроз и атак на веб-ресурсы.

В первую очередь, можно отметить классификацию консорциума WASC по угрозам безопасности и атакам на веб-ресурсы – *WASC Threat Classification*[14], *статистику открытого проекта OWASP по десяти самых опасным нарушениям и атакам на веб-приложения – OWASP Top 10*

[13] https://www.whitehatsec.com/info/website-stats-report-2016-wp/

[14] http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

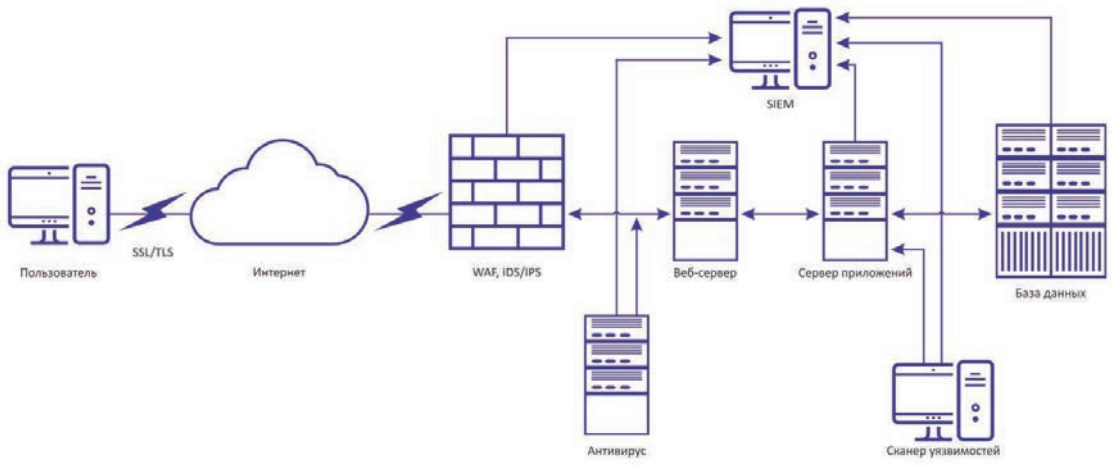

Рис. 4. Пример схемы веб-портала в защищенном исполнении

Таблица 6. Десять наиболее опасных нарушений и атак на веб-ресурсы (по оценке WASC)

№	Наименование	Комментарий
A1	Injection	Атаки класса инъекций, например: SQL-, OS-, XXE-, LDAP-инъекции и др.
A2	Broken Authentication and Session Management	Нарушение механизма аутентификации и правил управления сессиями
A3	Cross-Site Scripting (XSS)	Атаки межсайтового скриптинга (интерпретируемого кода), XSS-атаки
A4	Broken Access Control	Нарушение контроля доступа
A5	Security Misconfiguration	Некорректная конфигурация механизмов безопасности
A6	Sensitive Data Exposure	Компрометация конфиденциальных (чувствительных) данных
A7	Insufficient Attack Protection	Недостаточная защита от вторжений
A8	Cross-Site Request Forgery (CSRF)	Атака межсайтовой подделки запроса (CSRF-атаки) [12]
A9	Using Components with Known Vulnerabilities	Использование компонентов с незакрытыми известными уязвимостями
A10	Underprotected APIs	Использование незащищенных (уязвимые) интерфейсов API, как правило: SOAP/XML, REST/JSON, RPC, GWT и др.

Таблица 7. Примеры описаний угроз и уязвимостей веб-ресурсов в БДУ ФСТЭК России

№	Наименование угроз и уязвимостей
УБИ.041	Угроза межсайтового скриптинга. Угроза заключается в возможности внедрения нарушителем вредоносного кода в веб-ресурс.
УБИ.042	Угроза межсайтовой подделки запроса. Угроза заключается в возможности отправки нарушителем ссылки на содержащий вредоносный код веб-ресурс.
BDU:2015-10929	Уязвимость веб-сервера Apache HTTP Server, позволяющая нарушителю обойти существующие ограничения доступа.
BDU:2016-00707	Уязвимость прокси-сервера nginx, позволяющая нарушителю вызвать отказ в обслуживании.
BDU:2016-00484	Уязвимость веб-сервера визуализации контроллеров BACnet/IP-сетей SAUTER moduWeb Vision, позволяющая нарушителю получить конфиденциальную информацию.
BDU:2016-00258	Уязвимости веб-сервера IniNet Solutions GmbH's SCADA Web Server, позволяющие нарушителю выполнить произвольный код.
BDU:2015-11479	Уязвимость веб-сервера IBM HTTP Server, позволяющая нарушителю выполнить произвольный код.
BDU:2016-00483	Уязвимость веб-сервера визуализации контроллеров BACnet/IP-сетей SAUTER moduWeb Vision, позволяющая нарушителю внедрить произвольный Веб- или HTML-код.
BDU:2014-00397	Уязвимость сервера управления IP-адресами NameSurfer, позволяющая злоумышленнику внедрить вредоносный код, взаимодействующий с веб-сервером злоумышленника. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер.

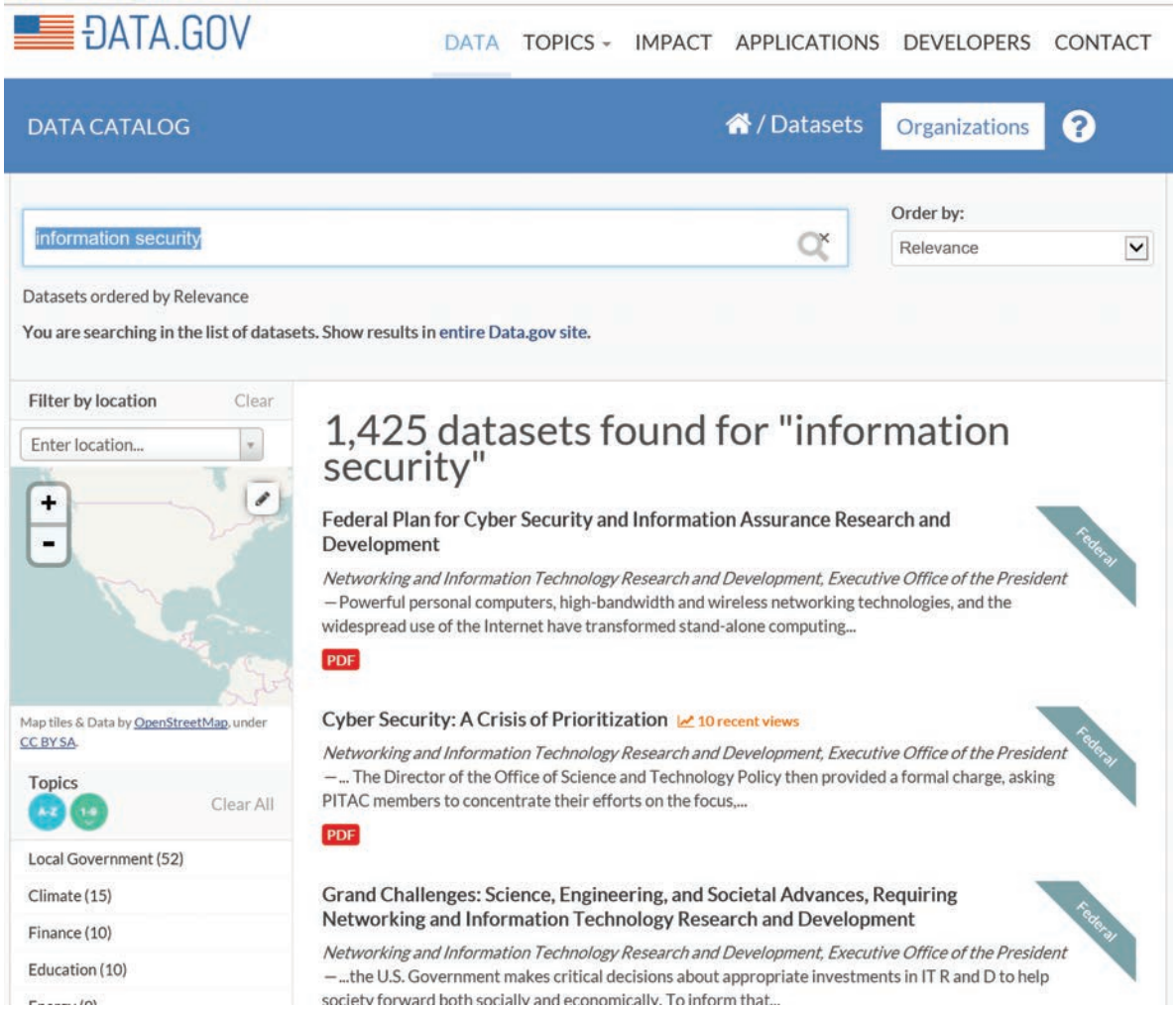

Рис. 5. Пример выполнения запроса на портале data.gov

Application Security Risks[15] *(табл. 6), а также шаблоны атак организации MITRE – CAPEC*[16]*, в том числе на веб-ресурсы.*

Банк данных угроз безопасности информации (БДУ) ФСТЭК России в настоящее время поддерживает известные угрозы веб-ресурсам и содержит актуальные уязвимости соответствующих приложений и платформ. Пример фрагмента угроз и уязвимостей БДУ ФСТЭК России продемонстрирован в табл. 7.

Послесловие

В завершение статьи хочется отметить текущее состояние использования ОД по информационной безопасности. Для иллюстрации ситуации весьма показательно сравнить порталы открытых данных США и РФ.

На рис. 5 приведен результат поискового запроса «INFORMATION SECURITY» на американском портале data.gov. Как видно из рисунка, система обнаружила в базе портала 1 425 наборов открытых государственных данных, востребованных в США. Заметим, что за прошедшие полгода база ОД по ИБ пополнилась новыми девятью десятками наборов ОД. Портал предоставляет различные фильтры поиска, в том числе по населенному пункту (англ. “filter by location”). Ради шутки был сделан запрос по месту расположения «Moscow» (на портале зафиксировано восемь небольших территориальных единиц США с глубоко историческим названием Moscow) – проверка показала, что по каждому указанному месту находится около сотни локальных наборов ОД по тематике, релевантной ИБ.

На рис. 6 представлен результат поискового запроса «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» на отечественном портале.

Из найденных строк (рис. 6) наиболее интересным, нам показалось, является третий (и последний) по порядку набор ОД. К сожалению, он оказался весьма лаконичным. Можно отметить стабильность интернет-портала: результаты авторского мониторинга портала в течение 6 месяцев не-

[15] https://www.owasp.org/index.php/Top_10_2017-Top_10
[16] https://capec.mitre.org

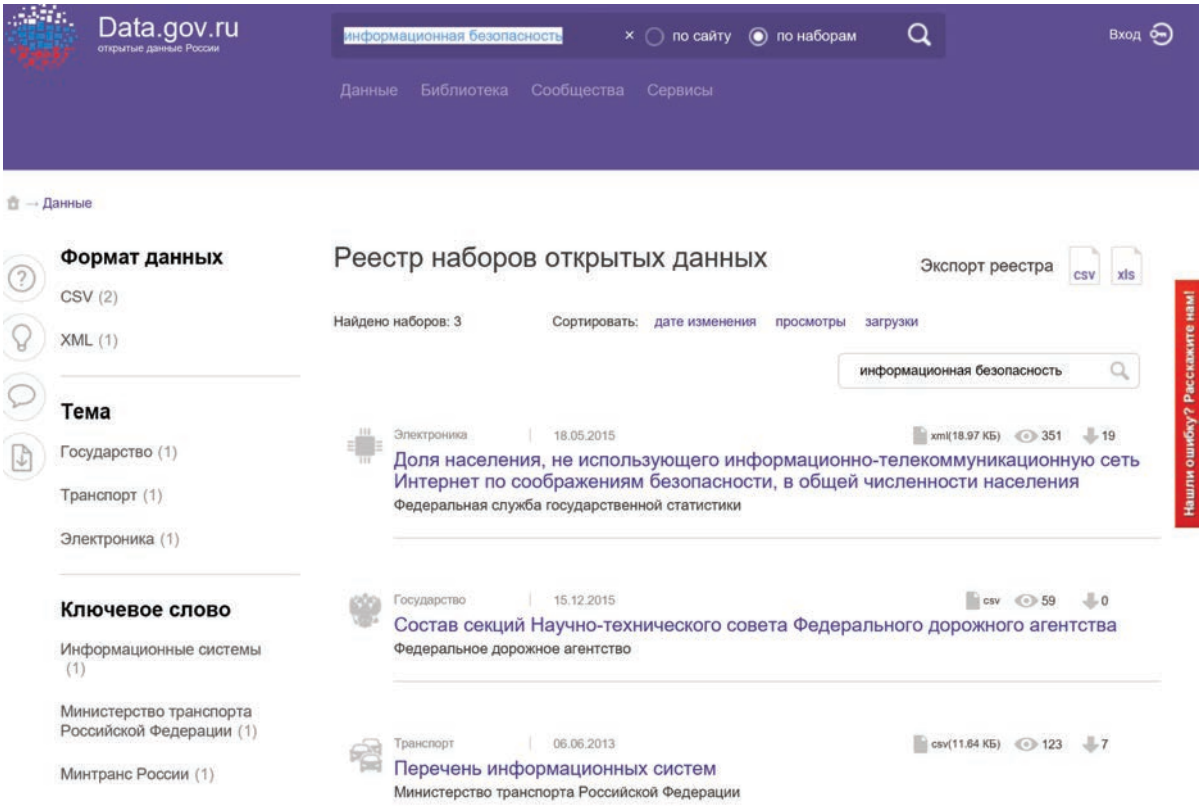

Рис. 6. Найденные по запросу наборы открытых данных на портале data.gov.ru

формально доказали строгое соответствие указанных ОД свойству инвариантности.

Представленный сравнительный анализ ставит **риторический вопрос о востребованности ОД в области ИБ** в нашей стране. На это есть несколько предположительных оправданий.

1. С политической точки зрения развитие системы ОД популизировались в период сотрудничества нашей страны в рамках Группы «Большой восьмерки», имеющей Хартию по теме (G8 Open Data Charter)[17], кстати, провозглашающей локальный принцип «Открытые данные по умолчанию». В настоящее время, по известным причинам, имеется некоторая настороженность, по крайней мере, в *симметричной* поддержке западных инициатив и методологий [13].

2. Несмотря на достаточный период инвестиций, – возможно, из-за отсутствия контура обратной связи – в стране еще не создали эффективную систему менеджмента жизненного цикла ОД по ИБ. Отмечается недостаточность сопутствующей методической базы и отсутствие института повышения квалификации персонала. Такая неопределённость, по оценкам ряда экспертов, приводит к снижению[18] мотивации сотрудников, поддерживающих такие системы [13–16]. Подобная проблема характерна для различных отраслей (в том числе и в ближайшем зарубежье [17–19]). Интересно исследование, проведенное, в частности, в налоговой сфере [20].

3. Силовые структуры РФ, на которые и возложено решение задач по информационной безопасности, заведомо достаточно консервативны, что обусловлено историческими объективными причинами и добрыми традициями.

Выводы

Проведенный анализ применения ОД в области ИБ в нашей стране позволяет сделать следующие выводы:

1. ОД являются примером «открытых» технологических инициатив, направленных не только на повышение эффективности государственного управления, но и на повышение эффективности исследований и производств продуктов и систем и в области ИБ.

2. ОД в техническом плане позволяют не только обеспечить ключевое требование менеджмента в области ИБ (согласно ГОСТ Р ИСО/МЭК 27001) по *информированности*, но и автоматизировать данный процесс благодаря открытым интерфейсам и форматам.

3. Основными угрозами ОД являются угрозы доступности и целостности, однако государствен-

[17] http://data.gov.ru/hartiya-otkrytyh-dannyh-gruppy-vosmi

[18] http://d-russia.ru/chislo-novyh-publikatsij-na-portale-otkrytyh-dannyh-rezko-snizilos-k-kontsu-2016-goda-eksperty.html

ные веб-порталы имеют широкий спектр современных угроз в информационной сфере, причем число компьютерных атак на веб-порталы неуклонно растет.

4. Вектор развития нормативной базы современных информационных систем обработки ОД и средств защиты ОД, а также стандартов и реестров угроз и уязвимостей веб-ресурсов, в целом определен, что упрощает деятельность разработчиков указанных систем.

5. В настоящее время ОД по ИБ (за исключением, может быть выделенных открытых данных ФСТЭК России), представлены в Рунет весьма скромно (см. рис.6). Например, пока нет ОД, касающихся работы государственных ситуационных центров по ИБ, и даже нет территориальной статистики по киберпреступлениям и киберзащищенности.

Можно предположить, что применение форматированных общедоступных данных в ИБ будет развиваться. Объективной причиной этого является появление новых информационных удобств (следовательно, и экономических выгод), сопутствующих информатизации общества и формированию безопасного виртуального киберпространства.

Рецензент: *Федичев Андрей Валерьевич, кандидат технических наук, директор Научного центра правовой информации при Минюсте России, Москва.*
E-mail: andrey.fedichev@scli.ru

Литература

1. Koznov D.V., Andreeva O., Nikula U., Maglyas A., Muromtsev D.I., Radchenko I. A Survey of Open Government Data in Russian Federation. In: IC3K 2016 – Proceedings of the 8th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management 8. 2016. P. 173-180.
2. Styrin E., Luna-Reyes L.F., Harrison T.M. Open Data and Open Government: from Abstract Principles to Institutionalized Practices. In: Proceedings of the 17th Annual International Conference on Digital Government Research – Internet Plus Government: New Opportunities to Solve Public Problems 2016. C. 76–85. DOI: http://dx.doi.org/10.1145/2912160.2912161.
3. Tauberer J. Open Government Data: 2nd Ed. Kindle Edition, 2014. 206 p.
4. Максименкова О.В., Подбельский В.В. Практика использования открытых данных в курсе «Программирование» образовательной программы бакалавриата «Программная инженерия» // Образование и наука. 2016. №10. С. 107–121. DOI: http://dx.doi.org/10.17853/1994-5639-2016-10-107-121.
5. Doroveev A.V., Markov A.S., Tsirlov V.L. Social Media in Identifying Threats to Ensure Safe Life in a Modern City // Communications in Computer and Information Science. 2016. V. 674. P. 441–449. DOI: http://dx.doi.org/10.1007/978-3-319-49700-6_44.
6. Бодрик А. Кибербезопасность открытых данных как предпосылка устойчивого развития цифровой экономики // PC Week/RE. 2016. № 20(919). 22 ноября 2016 г. 1 с.
7. Mendel T., Blanton T.S., Wadham J., et al., National Security and Open Government: Striking the Right Balance, preface by Alasdair Roberts, Campbell Public Affairs Institute, Maxwell School of Citizenship and Public Affairs, Syracuse University, 2003, 224 pp.
8. Scassa T. Privacy and Open Government. Future Internet, 2014, vol. 6, no. 2 (Open Government Meets Social Data), pp. 397-413. DOI: http://dx.doi.org/10.3390/fi6020397.
9. Radchenko I., Sakoyan A. The View on Open Data and Data Journalism: Cases, Educational Resources and Current Trends // Communications in Computer and Information Science. 2014. V. 436. P. 47-54.
10. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под. ред. А.С.Маркова. М.: Радио и связь, 2012. 192 с.
11. Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In: ACM International Conference Proceeding Series 8. Ser. Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015. 2015. P. 30-33. DOI: http://dx.doi.org/10.1145/2799979.2799980.
12. Барабанов А.В., Лавров А.И., Марков А.С., Полотнянщиков И.А. Исследование атак типа «межсайтовая подделка запросов» // Вопросы кибербезопасности. 2016. № 5 (18). С. 43–50.
13. Кабанов Ю.А., Карягин М.Е. «Необитаемые острова» открытости: проблемы открытых государственных данных в России // Политическая экспертиза: ПОЛИТЭКС. 2015. Т. 11. № 4. С. 38–51.
14. Бегтин И.В. Темная сторона открытости данных // Индекс безопасности. 21 (2015). № 3 (осень). С. 135–140.
15. Волков А.И., Рейнгольд Л.А. Открытые данные: проблемы и решения // Прикладная информатика. 2014. № 3 (51). С. 5–12.
16. Заборников А.Е. Открытые данные: риски и проблемы информационной безопасности // Научно-методический электронный журнал Концепт. 2017. Том 39 (май). С. 3881–3885.
17. Кунцевич С.С., Гедранович А.Б. Перспективы развития электронных государственных услуг в республике Беларусь // Актуальные проблемы науки XXI века. 2015. № 4. С. 36–41.
18. Самыкбаева Л.А. Открытые данные как фактор экономического развития страны // М. Рыскулбеков атындагы Кыргыз экономикалык университетинин кабарлары. 2016. № 2. С. 160–162.
19. Хохлов Ю.Е. Электронное государственное управление в странах СНГ // Информационное общество. 2016. № 4–5. С. 81–91.
20. Викторова Н.Г., Яблоков Д.Ю. Открытые данные в налогообложении: отечественная и зарубежная практика применения // Известия Уральского государственного экономического университета. 2016. № 2 (64). С. 21–30.