УДК 004.056
DOI 10.17150/2072-0904.2015.6(3).21

Д. И. Сачков
Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация
И. Г. Смирнова
Байкальский государственный университет экономики и права, г. Иркутск, Российская Федерация
В. Н. Быкова
ООО «ПИРАМИДА», г. Ангарск, Российская Федерация

ОЦЕНКА ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. Стремительное развитие телекоммуникационных и информационных технологий, а также повсеместное применение вычислительной техники привели к тому, что Интернет прочно вошел в жизнь современного человека. Социальные сети, интернет-магазины, развлекательные игры, портал государственных услуг, интернет-банкинг — вот далеко не полный перечень информационных продуктов, используемых сегодня. Эта сторона медали, позволяющая современному человеку экономить время. Как известно, есть и другая сторона медали — информационная безопасность человека, использующего телекоммуникационные технологии. В связи с многочисленными сообщениями об утечках персональных данных, их защита является приоритетным направлением не только со стороны государства, но и со стороны организаций всех форм собственности. Зная основные каналы утечки персональных данных в различных странах, операторы персональных данных могут предотвратить их незаконное распространение, копирование и сбор.

Ключевые слова. Киберпреступления; персональные данные; закон; защита информации; информационные системы; безопасность.

Информация о статье. Дата поступления 26 марта 2015 г.; дата принятия к печати 14 апреля 2015 г.; дата онлайн-размещения 5 мая 2015 г.

Финансирование. Государственное задание на выполнение проекта «Повышение эффективности уголовного судопроизводства по делам о киберпреступлениях для обеспечения национальной безопасности» в рамках гранта Президента Российской Федерации для государственной поддержки молодых российских ученых — докторов наук (Конкурс — МД-2014) на 2014-2015 годы (договор № 14.Z56.14.2691-МД).

D. I. Sachkov
Baikal State University of Economics and Law, Irkutsk, Russian Federation
I. G. Smirnova
Baikal State University of Economics and Law, Irkutsk, Russian Federation
V. N. Bykova
JSC «Piramida», Angarsk, Russian Federation

ASSESSMENT OF PERSONAL DATA PROTECTABILITY IN INFORMATION SYSTEMS

Abstract. Rapid development of telecommunication and information technologies, as well as total application of computing technology have resulted in the

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

fact that the Internet has come to stay in modern humans' life. The social nets, the Internet-shops, the entertaining games, the governmental service portal, the Internet banking — all these is not a complete list of information products used today. This is the side of the medal that allows the modern human to save time. As is known, there is the other side of the medal — the information security of the human that uses telecommunication technologies. In connection with many reports about leakage of personal data, their protection is a priority direction not only on part of the state but also on part of organizations of all types of property. Being aware of the main channals of personal data leakage in various countries, the personal data operators can prevent their illegal distribution, copying and collection.

Keywords. Cyber crimes; personal data; law; information protection; information systems; security.

Article info. Received March 26, 2015; accepted April 14, 2015; available online May 5, 2015.

Financing. The material was prepared in the framework of implementing the agreement on the conditions of using of the grant of the President of the Russian Federation for the state support of young Russian scientists with organizations — participants of the competition, having work relationship with young scientists No. 14.Z56.14.2691-MD (MD-2691.2014.6).

Проблемы информационной безопасности, защиты персональных данных (ПДн), обеспечения сохранности сведений, образующих охраняемую законом тайну, и иные аналогичные вопросы вызывают серьезную озабоченность всего мирового сообщества. Указанные явления самым непосредственным образом образуют угрозу национальной безопасности государств.

Так, по данным Главного информационного центра МВД России, в 2004 г. было совершено 13 723 компьютерных правонарушений, что почти в 2 раза больше (7 053) по сравнению с 2003 г., и их количество неуклонно растет. По словам руководителя Бюро специальных технических мероприятий МВД России А. Мошкова, в сфере высоких технологий именно мошенничества являются самыми распространенными преступлениями в IT-среде. Если в 2010 г. было возбуждено 736 таких уголовных дел, то за 9 месяцев 2011 г. их число уже превысило 1 тыс., при этом у данных преступлений весьма высокий уровень латентности [6; 7].

Не менее тревожные тенденции характеризуют состояние преступности и в странах Азиатско-Тихоокеанского региона. В частности, в Японии рекордное количество преступлений, связанных с Интернетом и другими компьютерными сетями, зафиксировано за прошедший год. Их количество увеличилось почти на треть и составило около 5 500 преступлений, среди которых большинство связано с присвоением денег в результате аукционных покупок по Интернету [5].

В соответствии с утвержденной Стратегией национальной безопасности Российской Федерации до 2020 г.[1] национальной безопасностью является состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства. В свою очередь, под угрозой национальной безопасности следует понимать прямую или косвенную возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию государства, его обороне и безопасности.

[1] Стратегия национальной безопасности Российской Федерации до 2020 года : указ Президента РФ от 12 мая 2009 г. № 537.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ
(Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА
Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

Совершение киберпреступлений самым непосредственным образом влияет на состояние защищенности жизненно важных интересов субъектов охраны. В этой связи необходимо отметить, что в соответствии со ст. 2 Конституции РФ права и свободы человека и гражданина являются высшей ценностью в государстве. К таковым относятся неприкосновенность личности, неприкосновенность жилища и, наконец, тайна (неприкосновенность) частной жизни, в том числе и ПДн [8]. И если во многих сферах государственной деятельности конфликт частных и публичных интересов неизбежен, то в случае совершения преступлений в сфере компьютерной информации в одинаковой степени страдают и частные интересы, и государственные, и общественные. Именно поэтому международно-правовое регулирование вопросов борьбы с киберпреступностью отличается разносторонностью и вариативностью.

В этой связи уместно вспомнить следующие нормативные акты международного характера:

1. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г.[1] Несмотря на то, что Российская Федерация не присоединилась к данной Конвенции, с точки зрения особенностей правового регулирования она представляет определенный интерес, поскольку устанавливает перечень преступлений, которые европейским сообществом отнесены к категории компьютерных. Так, к правонарушениям в сфере компьютерной информации отнесены: противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторского права и смежных прав. Как видно из приведенного перечня, в отличие от Уголовного кодекса РФ понятие компьютерных преступлений в данном акте толкуется расширительно.

2. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем от 28 января 2003 г.[2] Данный акт еще более расширяет сферу совершения компьютерных преступлений, относя к ним: распространение расистских и ксенофобских материалов посредством компьютерных систем, мотивированную угрозу расизма и ксенофобии, расистское и ксенофобское мотивированное оскорбление, отрицание, чрезвычайную минимизацию, одобрение или оправдание геноцида или преступлений против человечества посредством использования компьютерных систем.

3. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.[3] Данный документ по причине того, что Российская Федерация является его участницей, представляет для нас повышенный интерес. В целях оптимизации борьбы с киберпреступностью стороны договорились о том, что признают в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния, совершенные умышленно:

---

[1] Convention on cybercrime (Budapest, 23 November 2001). URL : conventions.coe.int/.../en/Treaties/Html/185.htm.

[2] Convention Committee on Cybercrime. URL : http://conventions.coe.int/Treaty/RUS/Treaties/Html/189.htm.

[3] Собрание законодательства РФ. 2009. № 13. Ст. 1460.

– осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

– создание, использование или распространение вредоносных программ;

– нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

– незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб[1].

4. Сообщение Европейской комиссии «На пути к общей политике по борьбе с киберпреступностью» от 22 мая 2007 г.[2]

5. Сообщение Европейской комиссии «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости» от 30 марта 2009 г.[3]

Особо следует подчеркнуть, что мировое сообщество в целом обеспокоено проблемами, связанными с таким явлением, как киберпреступность, а также с разработкой системы адекватных ответных мер со стороны всего мирового сообщества. В частности, в феврале 2013 г. в Вене группой экспертов был подготовлен итоговый документ, резюмирующий основные проблемы в сфере борьбы с киберпреступностью в различных государствах на всех континентах. Условно их можно разделить на 3 основные группы [12]:

Проблемы законодательного характера:

– отсутствие единого, универсального определения киберпреступности. В целом, предлагают следующую типологизацию компьютерных преступлений: сетевая атака и повреждение компьютерной системы; сетевое мошенничество; хищение денежных средств из финансовых учреждений путем несанкционированного доступа к компьютерным системам; азартные игры в онлайновой среде и реклама услуг сексуального характера в Интернете; посягательства на авторские и смежные права, преступления против интеллектуальной собственности; хищение информации, составляющей государственную тайну — угроза государственной безопасности; распространение информации;

– различный подход государств к определению круга составов преступлений, охватываемых понятием киберпреступности. Так, например, в Уголовном кодексе КНР было предусмотрено 5 статей, оговаривающих уголовную ответственность за компьютерные преступления. Постановлением Постоянного комитета ВСНП КНР об обеспечении безопасности Интернета[4], принятом в 2000 г., установлена уголовная ответственность уже за 15 видов компьютерных преступлений;

---

[1] Определение понятий «существенный вред», «тяжкие последствия» и «существенный ущерб» относится к компетенции Сторон.

[2] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 «Towards a general policy on the fight against cyber crime». URL : ec.europa.eu/…/docs/Communication_en.pdf.

[3] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience» of 30 march 2009. URL : ec.europa.eu/…/docs/Communication_en.pdf.

[4] Постановление Постоянного комитета ВСНП КНР об обеспечении безопасности в сети Интернет : принято 28 дек. 2000 г. 19 заседанием 9 созыва ПК ВСНП. URL : http://chupanov.narod.ru/Chinalaw/04/11.htm.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

– несмотря на возросшую за последнее десятилетие активность в принятии международных и региональных документов, направленных на противодействие киберпреступности (Совет Европы и Европейский Союз, СНГ или Шанхайская организация сотрудничества, межправительственные африканские организации, Лига арабских государств и ООН), во многих из них отсутствуют основные положения и имеются существенные расхождения;

– многие страны Азии считают свое действующее уголовно-процессуальное законодательство частично достаточным или недостаточным для расследования киберпреступлений [3].

Проблемы уголовно-процессуального характера:

– отсутствие четкого определения диапазона специальных следственных полномочий в сфере международного сотрудничества при производстве по данной категории уголовных дел;

– недостаточность уровня подготовки прокуроров для работы с электронными доказательствами и отстаивания своей процессуальной и правовой позиции в суде, которую отмечают все страны Африки, а также треть иных стран. Аналогичным образом только в каждой десятой стране существуют специализированные судебные службы. Например, 19 мая 2014 г. премьер-министр Японии С. Абэ на заседании правительственного комитета по информационной безопасности отметил, что в связи с ростом угроз киберпространству одной из ответных мер станет превращение нынешнего комитета по информационной безопасности в комитет по кибербезопасности с приданием ему дополнительных функций, а также будет учреждена должность чиновника по кибербезопасности при правительстве в статусе заместителя министра. Он должен будет координировать действия и информацию между государственными структурами, частными компаниями, а также с другими государствами[1]. В свою очередь, в Китае для борьбы с компьютерной преступностью созданы специальные отряды «интернет-полиции».

Проблемы криминалистического характера имеют преимущественно организованный характер совершаемых киберпреступлений. Одно из самых распространенных явлений «фишинг» представляет собой охоту за ПДн клиентов в Интернете. Как правило, кибер-преступники используют ложную электронную почту и сайты, чтобы обмануть пользователя и заполучить его личную информацию. Пользователям Интернета, чтобы не попасться на удочку мошенников, советуется почаще менять пароли и идентификационные коды.

Можно упомянуть также необычную форму кибернетической преступности со стороны Китайской Народной Республики. Продукция, поступающая с китайских заводов, в большинстве случаев начиняется шпионскими приспособлениями, а если речь идет об электронике, то она изначально заражена вредоносным программным обеспечением или так называемыми «вирусными программами». Все чаще и чаще внутри китайской продукции находят подозрительные комплектующие. При этом продукция, в которой были найдены шпионские устройства, варьируется от флеш-карт и мелкой бытовой техники, например, блендеров и чайников, до крупной домашней электроники, такой как телевизоры, домашние кинотеатры и компьютеры[2].

Организованный характер кибер-угроз подтверждается также выступлением генерала Сон Юн Кын, занимающегося в вооруженных силах Республи-

[1] РИА новости. URL : http://rian.com.ua/world_news/20140519/349471767.html?utm_source=twitterfeed&utm_meium=twitter.

[2] China modern. URL : http://www.chinamodern.ru/?p=13939.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

ки Корея вопросами национальной безопасности, в котором генерал утверждает, что северокорейские компьютерные взломщики уже активно проникают в южнокорейские компьютерные сети. Особенно хакеров из КНДР привлекают сети государственных ведомств, из которых разведчики пытаются красть секретные сведения[1].

Многогранность существующих проблем требует незамедлительной реакции государств на вызовы преступного мира в виртуальном пространстве. На наш взгляд, первоочередной задачей в данном случае должна стать качественная оценка защищенности ПДн в информационных системах, так как ПДн отнесены к категории конфиденциальной информации, доступ к которой ограничен законодательством[2]. Однако все чаще в средствах массовой информации появляются сведения об утечках ПДн клиентов, сотрудников. Уже никого не удивляют сообщения о краже паспортных данных сотрудниками банка для совершения мошеннических действий [11].

Для определения класса информационной системы необходимо выполнение двух требований: определить категории ПДн и количество субъектов ПДн. Процедура их категорирования является трудно формализованной задачей, так как в нормативных документах отсутствует точный перечень ПДн. Исходя из имеющихся нормативно-правовых документов, ПДн возможно разделить на 4 категории: О — общедоступные данные; И — иные категории персональных данных; Б — биометрические персональные данные; С — специальные персональные данные (табл.).

Категорирование персональных данных

№	Персональные данные	Категория
a	Фамилия, имя, отчество	О
b	Паспортные данные	И
c	Дата и место рождения	И
d	ИНН, СНИЛС	И
e	Телефоны (домашний, мобильный)	О
f	Адрес (фактический, по прописке)	И
g	Электронная почта	О
h	Военный билет, паспорт моряка, временное удостоверение	И
j	Номер водительского удостоверения	И
k	Сведения о доходе, номера банковских карт, финансовое состояние	И
l	Семейное положение, наличие детей	И
m	Фотография	Б
n	Состояние здоровья/сведения об инвалидности	С
o	Информация о национальности, расовой принадлежности	С
p	Информация о политических взглядах	С
q	Данные о религиозных убеждениях	С
r	Данные об интимной жизни	С
s	Другие данные: образование, повышение квалификации, курсы, льготы и др.	И

В проанализированных работах и методиках на предмет категорирования ПДн [1; 2; 4; 9] не существует единой точки зрения на однозначное определе-

[1] Центр исследования компьютерной преступности. URL : http://www.chinamodern.ru/?p=13939.

[2] О персональных данных : федер. закон РФ от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31. Ч. 1. Ст. 3451.

ние категории. Для идентификации субъекта необходимо определить соответствующие признаки. Для этого имеющиеся ПДн можно разделить на несколько групп:

– A — общедоступные данные, которые включают в себя множество $A = \{a, e, o\}$. По данным признакам идентифицировать однозначно невозможно;

– B — иные категории ПДн, по которым можно однозначно идентифицировать субъекта ПДн, содержит множество $B = \{b, d, h, j\}$;

– C — биометрические ПДн, по которым можно опознать человека, содержатся в множестве $C = \{m\}$;

– D — специальные категории ПДн, включающие информацию о расовой, национальной принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья, интимной жизни, но не позволяющие однозначно идентифицировать гражданина. Содержатся во множестве $D = \{n, o, p, q, r, s\}$;

– E — иные категории ПДн, не позволяющие однозначно идентифицировать гражданина, содержатся во множестве $E = \{c, k, l, s\}$.

Для определения категории персональных данных их необходимо определить в соответствующие множества:

– ИСПДн-О — множество A (рис. 1 а);

– ИСПДн-Б — множества $A \cup C$ и $C \cup B$ (рис. 1 б);

– ИСПДН-И — множества $A \cup B$; $A \cup E$; $E \cup B$ (рис. 1 в);

– ИСПДн-С — множества $A \cup D$, $D \cup B$, $C \cup D$; $E \cup D$ (рис. 1 г).

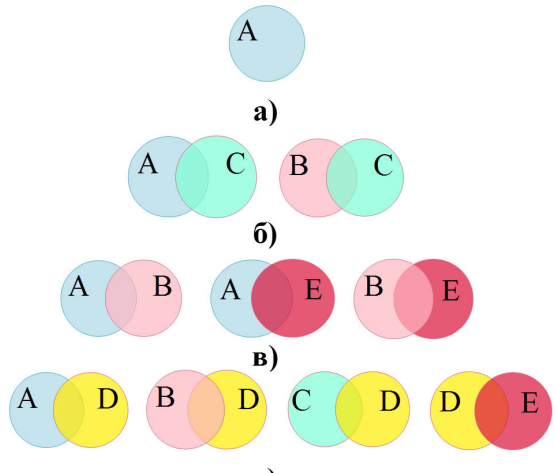

Рис. 1. Определение типа информационной системы персональных данных

На основе данного категорирования разработан алгоритм (рис. 2), позволяющий сэкономить время оператора ПДн при определении класса информационной системы персональных данных (ИСПДн). Данный алгоритм также позволяет определить уровень защищенности информационной системы и в дальнейшем быстро перейти на следующий этап, который выявляет тип угроз и уязвимостей информационной системы.

Для более эффективной оценки защищенности персональных данных на предприятиях малого и среднего бизнеса необходимо использование методики оценки уровня защищенности ПДн [10], предназначенной для того, чтобы руководители и специалисты компании могли без дополнительных материальных и временных затрат выполнить требования законодательства по защите ПДн.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ
(Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА
Baikal Research Journal
http://eizvestia.isea.ru
2015. Т. 6, № 3

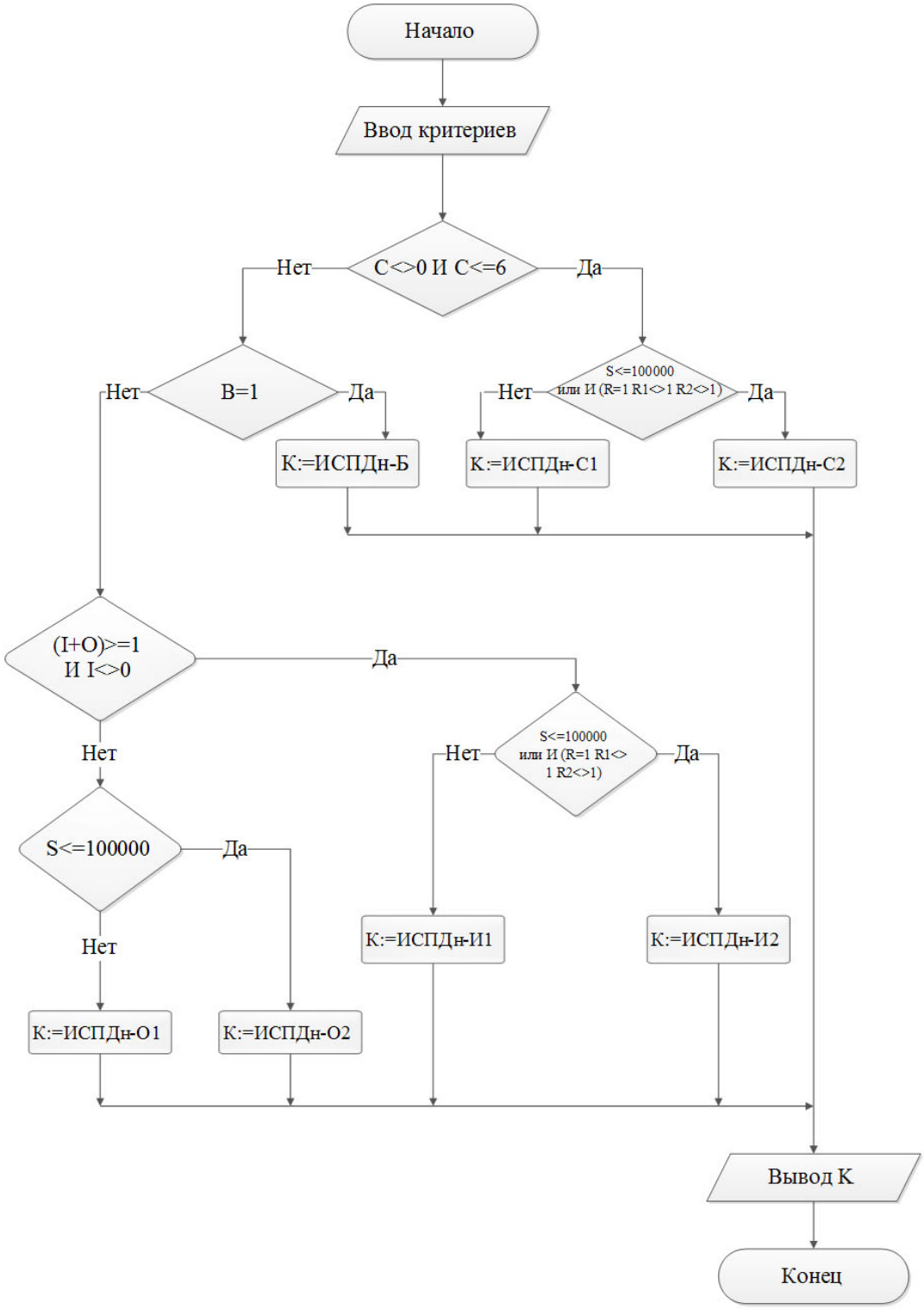

Рис. 2. Алгоритм определения типа информационной системы персональных данных

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
http://eizvestia.isea.ru
2015. Т. 6, № 3

Модель процесса оценки защищенности ИСПДн (рис. 3) основывается на методических документах[1], построена в процессе интервьюирования различных специалистов(руководителей, бухгалтеров, системных администраторов, других специалистов) и состоит из опросного листа, который, в свою очередь, разбит на группы, позволяющие оценить уровень защищенности ПДн [1]:

– требования по программной защите;

– требования по технической защите (утечки по техническим каналам; угрозы несанкционированного доступа);

– требования по организационной защите;

– класс ИСПДн (категории ПДн, объем ПДн);

– уровень защищенности (модель нарушителя; типы угроз; базовые модели угроз).

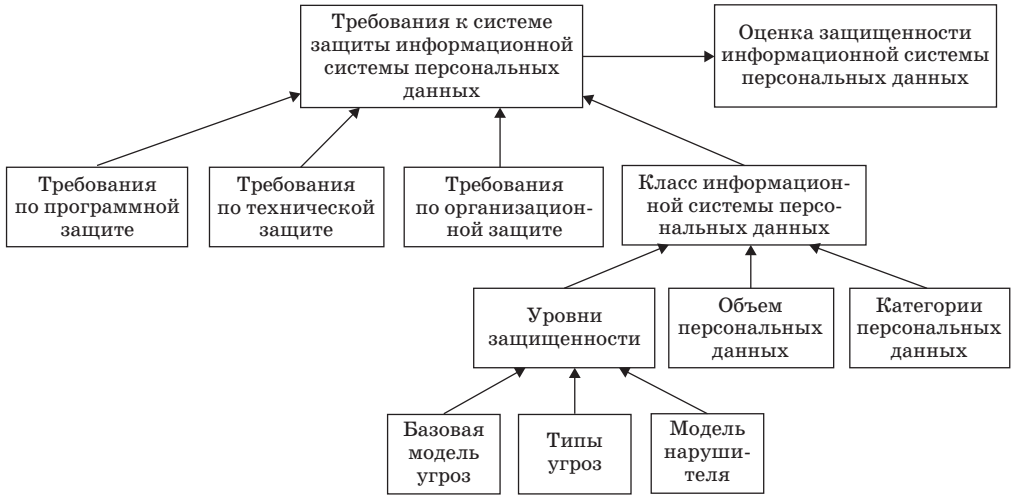

Рис. 3. Сетевая модель процесса оценки защищенности информационной системы персональных данных

При оценке общего уровня защищенности ИСПДн следует отметить, что соблюдение всех перечисленных требований является необходимым условием для безопасного функционирования информационной системы. Все показатели по группам оформляются в таблицу с вычисленным уровнем показателя по каждой группе, а оценка общего уровня защищенности ИСПДн производится по следующим пунктам:

а) ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

б) ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

в) ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты а и б.

[1] Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февр. 2013 г. № 21; Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : утв. ФСТЭК России от 14 февр. 2008 г.; Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : утв. ФСТЭК России от 15 февр. 2008 г.

О защищенности информационной системы можно судить, если осуществляются все организационные, технические и правовые требования[1].

Конфиденциальная информация, к которой относятся ПДн, должна обрабатываться в помещениях с ограниченным доступом, видеонаблюдением, надежной антивирусной системой, при отсутствии возможности распечатывать документы, не санкционированно их копировать и загружать со сменного носителя — только совокупность этих мер приведет к высокой оценке защищенности ПДн[2].

Основной задачей в настоящий момент является снижение трудоемкости и повышение эффективности защиты ПДн, обрабатываемых в информационных системах, на что и направлен предлагаемый алгоритм категорирования ПДн, позволяющий с минимальными временными затратами определить их категорию. Данный алгоритм поможет исключить неоднозначность определения категории ПДн, выявить тип информационной системы и тип актуальных угроз. Подспорьем для алгоритма категорирования может служить методика оценки уровня защищенности ПДн на основе нормативных документов. Она позволит объективно оценить насколько организация выполняет требования законодательства и принять меры по устранению недостатков.

Список использованной литературы

1. Голеомбиовская О. М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : дис. ... канд. техн. наук : 05.13.19 / О. М. Голеомбиовская. — Брянск, 2013. — 167 с.

2. Голеомбиовская О. М. Разработка автоматизированной системы аудита и построения модели объекта защиты с использованием технологии 3D-прототипирования / О. М. Голеомбиовская, М. В. Терехов // Материалы II Региональной научно-практической конференции «Региональные проблемы защиты персональных данных». — Брянск : Брян. гос. техн. ун-т, 2010. — С. 47–49.

3. Егерева О. А. Некоторые проблемы, возникающие при расследовании преступлений в сфере компьютерной информации и компьютерных сетях: к вопросу о криминалистическом аспекте собирания доказательств / О. А. Егерева, И. Г. Смирнова // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства : материалы междунар. науч.-практ. конф. Иркутск, 25–26 сент. 2014 г. — Иркутск : Изд-во БГУЭП, 2014. — С. 337–343.

4. Жук Р. В. Классификация информационных систем персональных данных: вчера, сегодня завтра / Р. В. Жук, А. В. Власенко // Известия Юго-Западного государственного университета. — 2013. — № 1. — С. 87–90.

5. Коломинов В. В. Мошенничество в сфере компьютерной информации: криминалистический аспект / В. В. Коломинов // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 1. — URL : http://eizvestia.isea.ru/reader/article.aspx?id=19976.

6. Львович Я. Е. Модель нарушителя информационной безопасности / Я. Е. Львович, Д. С. Яковлев // Промышленные АСУ и контроллеры. — 2012. — № 2. — С. 54–56.

7. Миронова В. Г. Модель нарушителя информационной безопасности / В. Г. Миронова, А. А. Шелупанов // Промышленные АСУ и контроллеры. — 2012. — № 3. — С. 53–56

8. Новиков В. А. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности / В. А. Новиков // Уголовное право. — 2011. — № 1. — С. 43–48.

9. Петренко С. А. Инфраструктурные модели операторов персональных данных / С. А. Петренко, А. В. Зотова // Защита информации. INSIDE. — 2013. — № 6. — С. 42–45.

[1] Об утверждении требований и методов по обезличиванию персональных данных : приказ Роскомнадзора от 5 сент. 2013 г. № 996 // Российская газета. 2013. № 208.

[2] Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февр. 2013 г. № 21.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru

10. Попова Е. В. Повышение конкурентоспособности малых предприятий сферы услуг путем усиления информационной безопасности после принятия закона о персональных данных / Е. В. Попова // Журнал правовых и экономических исследований. — 2012. — № 3. — С. 106–110.

11. Сачков Д. И. Использование информационных систем для защиты персональных данных // Д. И. Сачков, В. Н. Быкова // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2014. — № 3. — С. 203–210. — URL : http://eizvestia.isea.ru/reader/article.aspx?id=19125.

12. Сачков Д. И. Обеспечение информационной безопасности в органах власти : учеб. пособие / Д. И. Сачков, И. Г. Смирнова. — Иркутск : Изд-во БГУЭП, 2015. — 122 с.

References

1. Goleombiovskaya O. M. *Avtomatizatsiya vybora sredstv zashchity personal'nykh dannykh na osnove analiza ikh zashchishchennosti. Kand. Diss.* [Automation of selecting personal data protection means on the basis of their protectability analysis. Cand. Diss.]. 2013. 167 p.

2. Goleombiovskaya O. M., Terekhov M. V. Development of automated audit system and of building of object protection model using the 3D prototyping technology. *Regional'nye problemy zashchity personal'nykh dannykh. Materialy II Regional'noi nauchno-prakticheskoi konferentsii* [Regional problems of personal data protection. Materials of 2nd Regional Research Conference]. Bryansk State Technical University (BSTU) Publ., 2010, pp. 47–49. (In Russian).

3. Egereva O. A., Smirnova I. G. Some problems arising in investigating crimes in computer information sphere and computer networks: on issue of criminalistics aspects of collecting evidences. *Ugolovno-protsessual'nye i kriminalisticheskie sredstva obespecheniya effektivnosti ugolovnogo sudoproizvodstva. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii. Irkutsk, 25–26 sentyabrya 2014 g.* [Criminal-procedural and criminalistic ways of providing efficiency of criminal procedure. Materials of International Science and Practice Conference. Irkutsk, Sept. 25–26, 2014]. Irkutsk, Baikal State University of Economics and Law Publ., 2014, pp. 337–343. (In Russian).

5. Zhuk R. V., Vlasenko A. V. Classification of personal date information systems: yesterday, today, tomorrow. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Izvestiya of Southwest State University,* 2013, no. 1, pp. 87–90. (In Russian).

6. Kolominov V.V., Fraud in the field of computer information: criminalistic aspect *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* (*Baykalskiy gosudarstvennyy universitet ekonomiki i prava*) = *Izvestiya of Irkutsk State Economics Academy* (*Baikal State University of Economics and Law*), 2015, vol. 6, no. 1. Available at: http://eizvestia.isea.ru/reader/article.aspx?id=19976. (In Russian).

7. L'vovich Ya. E., Yakovlev D. S. Model of violator of information security. *Promyshlennye ASU i kontrollery = Industrial Automated Control Systems and Controllers,* 2012, no. 2, pp. 54–56. (In Russian).

8. Mironova V. G., Shelupanov A. A. Model of a violator of information security. *Promyshlennye ASU i kontrollery= Industrial Automatied Control Systems and Controllers*, 2012, no. 3, pp. 53–56. (In Russian).

9. Novikov V. A. The concept of private life and criminal-legal protection of its immunity. *Ugolovnoe pravo = Criminal law*, 2011, no. 1, pp. 43–48. (In Russian).

10. Petrenko S. A., Zotova A. V. Infrastructural models of personal date operators *Zashchita informatsii. INSIDE = Information Protection. INSIDE*, 2013, no. 6, pp. 42–45. (In Russian).

11. Popova E. V. Improving competitiveness of small service businesses through strengthening information security after adoption of the personal data law. *Zhurnal pravovykh i ekonomicheskikh issledovanii = Journal of Legal and Economic Studies,* 2012, no. 3, pp. 106–110. (In Russian).

12. Sachkov D. I., Bykova V. N. Use of information systems for personal data protection. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* (*Baykalskiy gosudarstvennyy universitet ekonomiki i prava*) = *Izvestiya of Irkutsk State Economics Acad-*

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
http://eizvestia.isea.ru
2015. Т. 6, № 3

emy (*Baikal State University of Economics and Law*), 2014, no. 3, pp. 203–210. Available at: http://eizvestia.isea.ru/reader/article.aspx?id=19125. (In Russian).

13. Sachkov D. I., Smirnova I. G. *Obespechenie informatsionnoi bezopasnosti v organakh vlasti* [Provision of information security in authority bodies]. Irkutsk, Baikal State University Economics and Law Publ., 2015. 122 p.

Информация об авторах

Сачков Дмитрий Иванович — кандидат экономических наук, доцент, начальник научного отдела, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: leninb@yandex.ru.

Смирнова Ирина Георгиевна — доктор юридических наук, заведующая кафедрой криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: smirnova-ig@mail.ru.

Быкова Вера Николаевна — магистр прикладной информатики, руководитель отдела интернет-технологий, ООО «Пирамида», 665824, г. Ангарск, 22 кв., 6, e-mail: Bykova.vn@yandex.ru.

Authors

Dmitry I. Sachkov — PhD in Economics, Assistant Professor, Head of Research Department, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russian Federation; e-mail: leninb@yandex.ru.

Irina G. Smirnova — Doctor habil. (Law), Head of Chair of Criminalistics and Forensic Enquiry, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russian Federation; e-mail: smirnova-ig@mail.ru.

Vera N. Bykova — Master Degree Student in Applied Computer Science, Head of Internet Technologies Department, JSC «Piramida», 22 Block, 6, 665824, Angarsk, Russian Federation; e- mail: Bykova.vn@yandex.ru.

Библиографическое описание статьи

Сачков Д. И. Оценка защищенности персональных данных в информационных системах / Д. И. Сачков, И. Г. Смирнова, В. Н. Быкова // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 3. — DOI : 10.17150/2072-0904.2015.6(3).21.

Reference to article

Sachkov D. I., Smirnova I. G., Bykova V. N. Assessment of personal data protectability in information systems. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* (*Baykalskiy gosudarstvennyy universitet ekonomiki i prava*) = *Izvestiya of Irkutsk State Economics Academy* (*Baikal State University of Economics and Law*), 2015, vol. 6, no. 3. DOI: 10.17150/2072-0904.2015.6(3).21. (In Russian).

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
НОВОЕ НАЗВАНИЕ ЖУРНАЛА Baikal Research Journal
2015. Т. 6, № 3
http://eizvestia.isea.ru