**Викторова Наталья Викторовна**

*доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, n.v.viktorova@utmn.ru*

**Каримова Диана Вильдановна**

*старший преподаватель кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, d.v.karimova@utmn.ru*

**Камнева Ангелина Владимировна**

*студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, kamneva.angelina@mail.ru*

**Огаркова Татьяна Сергеевна**

*студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, ts.fefilova@gmail.com*

**Титаренко Диана Александровна**

*студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, hpp2dz@gmail.com*

# РИСКИ И УГРОЗЫ ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В БАНКАХ И АЭРОПОРТАХ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ

**Аннотация.** Статья посвящена выявлению рисков и угроз, связанных с использованием персональных данных в банковской и авиатранспортной сферах в условиях цифровизации экономики, а также основным методам совершения кибератак на данные сферы. На сегодняшний день развитие цифровой экономики, безусловно, способствует возникновению новых преимуществ и возможностей, но в то же время становится причиной возникновения новых угроз, из которых самыми опасными признаются киберугрозы.

**Ключевые слова:** персональные данные, цифровизация экономики, киберпреступность, риски и угрозы.

**Viktorova Natalia Viktorovna**

*Associate Professor of the Department of Economic Security, System Analysis and Control at Tyumen State University, Tyumen, n.v.viktorova@utmn.ru*

**Karimova Diana Vildanovna**

*Senior lecturer of the Department of Economic Security, System Analysis and Control at Tyumen State University, Tyumen, d.v.karimova@utmn.ru*

**Kamneva Angelina Vladimirovna**

*Student of the specialty "Economic Security" at Tyumen State University, Tyumen,*

*kamneva.angelina@mail.ru*

**Ogarkova Tatiana Sergeevna**

*Student of the specialty "Economic Security" at Tyumen State University, Tyumen,*

*ts.fefilova@gmail.com*

**Titarenko Diana Alexandrovna**

*Student of the specialty "Economic Security" at Tyumen State University, Tyumen,*

*hpp2dz@gmail.com*

# RISKS AND THREATS OF USING PERSONAL DATA IN BANKS AND AIRPORTS IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF THE ECONOMY

**Abstract.** The article is devoted to identifying risks and threats associated with the use of personal data in the banking and air transport sectors in the context of the digitalization of the economy, as well as the main methods of carrying out cyberattacks on these areas. Today, the development of the digital economy undoubtedly contributes to the emergence of new advantages and opportunities, but at the same time it becomes the cause of the emergence of new threats, of which cyber threats are recognized as the most dangerous.

**Keywords:** personal data, digitalization of the economy, cybercrime, risks and threats.

Ключевым и самым востребованным активом цифровой экономики является информация, исходя из чего, различные данные (учетные, персональные, коммерческая тайна и др.) являются весьма ценным ресурсом. Однако особое внимание следует акцентировать на персональных данных, к которым относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1], поскольку именно их получение является ведущим мотивом киберпреступников.

Количество киберинцидентов в России за каждый месяц первой половины 2020 г. уже превышает показатели аналогичных периодов 2019 г. (рисунок 1). Число атак во 2 квартале 2020г. по сравнению с 1 кварталом выросло на 9%, а по сравнению с аналогичным периодом 2019 года - на 59%.

Представленные данные свидетельствуют о наличии тенденции к росту числа совершаемых киберпреступлений, обусловленной расширением масштабов цифровизации.

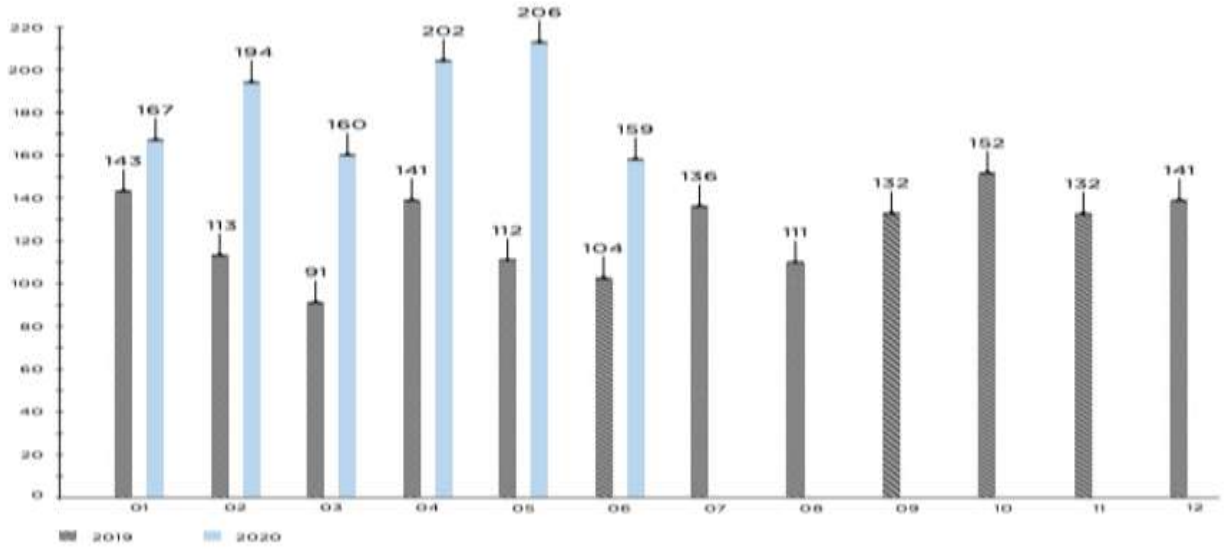


Рисунок 1. Количество киберинцидентов в России

Источник: [2]

Безусловно, основной причиной такого роста стала известная всем эпидемиологическая и экономическая ситуация в мире, которая создала весьма благоприятную почву для кибермошенников при переводе большей части сфер жизнедеятельности общества в онлайн-среду. Данный вывод подтверждает и статистика, поскольку именно на апрель и май 2020 г. приходилось рекордное число успешных кибератак, по большей части совершаемых с использованием методов социальной инженерии либо распространением вирусного программного обеспечения (рисунок 2).

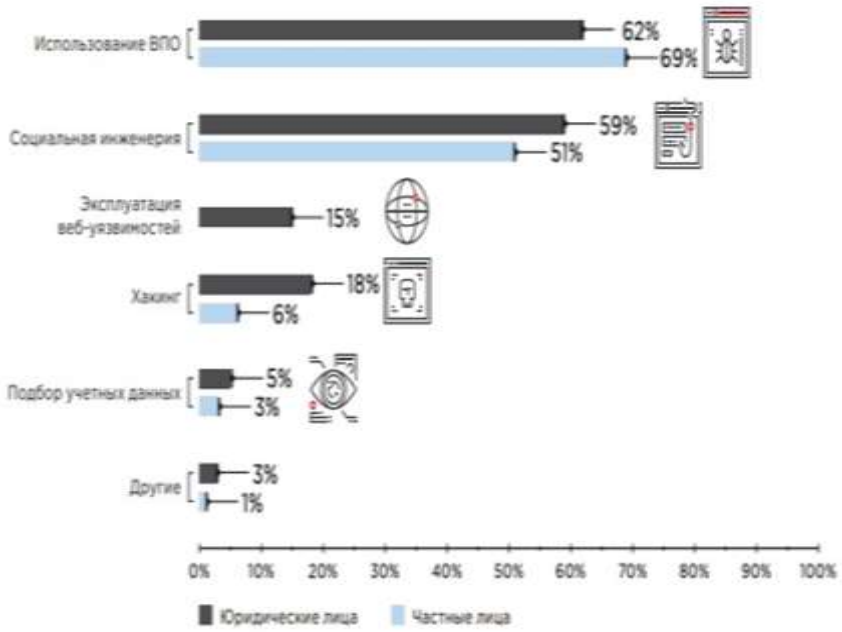


Рисунок 2. Применяемые методы кибератак в России (первое полугодие 2020 г.)

Источник: [2]

В настоящее время ни для кого не секрет, что главной целью злоумышленников чаще всего является получение финансовой выгоды. Однако мало кто задумывается над тем, что мотивы преступников трансформируются вместе с развитием окружающей среды. Цифровизация экономики, ключевым активом которой является информация, привела к тому, что на сегодняшний день ведущим мотивом киберпреступников является получение данных (рисунок 3).

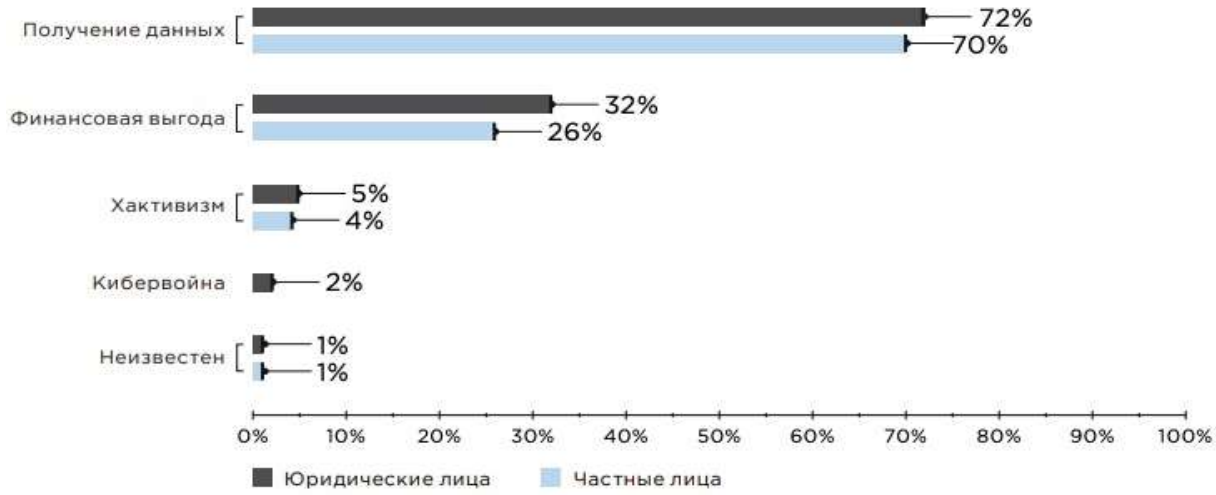


Рисунок 3. Мотивы киберпреступников в России (первая половина 2020 г.)

Источник: [2]

По данным Всемирного экономического форума кража данных занимает в системе глобальных рисков (с точки зрения вероятности их возникновения) 4 место, что, безусловно, требует безотлагательных мер по ее предотвращению [3].

В период с 2017 по 2019 год статистика хищений персональных данных заняла центральное место среди многих статистических данных, охватывающих сферу киберпреступности. Среди зарегистрированных в 2019 году случаев утечек информации доля утечки персональных данных в России превысила показатели зарубежных стран более чем на 10% (рисунок 4).


Рисунок 4. Распределение утечки информации по видам в России и мире в 2019 г.

Источник: [4]

Важно отметить, что осуществить и монетизировать кражу или утечку личных данных на сегодняшний день является достаточно просто. Номера кредитных карт, паспортные данные и иные персональные данные могут быть украдены и проданы в сети Интернет или использованы преступниками для быстрого и легкого получения прибыли [5].

Заполучив, например, паспортные данные злоумышленники могут воспользоваться ими следующим образом:

– оформить кредит в кредитной организации или оформить онлайн-займ;

– открыть счёт через онлайн-систему, получив пластиковую карту;

– зарегистрироваться в онлайн-казино и повесить на владельца данных внушительные долги;

– осуществить регистрацию компании или ИП;

– подписать сделку купли-продажи недвижимости;

– приобрести сим-карты;

– получить доступ к соцсетям и номеру телефона владельца данных.

При этом риск мошенничества существует не только при использовании мошенниками паспортных данных, но и данных СНИЛСа, свидетельства о рождении, медицинского полиса. Для этого им достаточно знать номер документа, дату его выдачи и рождения владельца, данные о регистрации [6].

В настоящее время объектом повышенного внимания злоумышленников по-прежнему остаются банки и иные финансовые организаций. Однако, учитывая достаточно высокую степень защищенности данных структур, кибератаки на кредитно-финансовую сферу все чаще осуществляются не одиночными хакерами, а хорошо организованными преступными группировками.

Применительно к кредитно-финансовой сфере главной целью мошенников, безусловно, остается получение прямой финансовой выгоды (65% инцидентов) [7]. Однако, важно отметить, что удельный вес краж данных растет еще более высокими темпами. Причиной этого является наличие финансового подтекста в преступлениях, направленных на получение данных, т.е. украденные данные в последующем также используются для хищения денежных средств.

Цифровизация экономики спровоцировала рост киберинцидентов, связанных с завладением информации о платежных картах, персональных и учетных данных пользователей для доступа к их личным кабинетам с целью совершения кражи денежных средств либо же продажи данной информации в Darknet. В настоящее время кража информации в финансовых организациях уже стала многофункциональным преступным бизнесом, с каждым годом набирающим свои обороты (54% IT-инцидентов против 30%

извлечения финансовой выгоды и 15% хактивизма), а пароли и логины от различных учетных данных и реквизиты банковских карт заняли порядка 80% всей информации, продаваемой в Darknet [7].

Данные, приобретаемые в DarkNet, являются для мошенников гарантией эффективного применения методов социальной инженерии, поскольку владение персональными данными позволяет им значительно повысить доверие потенциальной жертвы. Так, в 2019 году доля социальной инженерии в общем объеме атак на банковскую сферу уже достигла 90% [8].

Самым популярным инструментом социальной инженерии является Vishing, представляющий собой вид атаки, при котором мошенники звонят на мобильные номера жертв и, притворяясь представителем легитимной организации (чаще всего банка), узнают конфиденциальную информацию. В данном случае тактика увязана с подделкой идентификатора вызывающего абонента, что позволяет добиться максимальной реалистичности и не вызвать подозрения жертвы. Важно отметить, что в настоящее время на Vishing приходится 9 совершаемых атак из 10, что, свидетельствует о достаточно низком уровне финансовой грамотности граждан [8].

Еще одним весьма известным инструментом социальной инженерии, доля которого в общей структуре атак на сегодняшний день достигает 3%, является фишинг [8]. Данные атаки осуществляются на базе электронной почты и направлены, как правило, на конкретного человека или всю организацию в целом. Главной целью фишинга является стремление побудить потенциальную жертву перейти по вредоносным ссылкам, предоставить свои учетные данные либо же иную личную информацию.

В 2019 г. достаточно распространенным было направление фишинга, связанное с рассылкой формальных писем сотрудникам банка якобы от HR-службы с требованием пройти аттестацию, перейдя по ссылке на указанный внешний сайт. Для большинства сотрудников данная процедура не вызывала сомнений, поскольку она является обязательной для многих банков и генерирует премиальные выплаты, составляющие большую часть дохода сотрудников. По данным исследования, проведенного BI.ZONE при учебной рассылке фишинговых писем 28% сотрудников открыли файл и разрешили запуск макроса, 35% перешли по ссылке и 18% ввели свои логин и пароль от рабочей почты [9].

В результате данной атаки злоумышленники получают доступ к переписке представителя банка с клиентами, как правило, содержащую файлы с их персональными данными, а также возможность выйти на диалог с клиентом и запросить необходимую информацию. Главным объектом направленности для мошенников в данном случае являются сотрудники департаментов, непосредственно связанных с обслуживанием клиентов, а именно:

выдачей кредитов, обслуживанием банковских карт, предоставлением дистанционного доступа, обработкой претензий.

Важно подчеркнуть, что в отношении финансовой сферы также особенно часто фишинг применяется для распространения вредоносного программного обеспечения, доля которого составляет порядка 27–30% совершаемых фишинговых рассылок. В целом на финансовую сферу приходится 65% случаев кибератак, связанных с распространением вредоносного ПО [7].

Таким образом, увеличение объемов кражи данных является на данный момент не просто предположением и возможной угрозой будущего, а реальностью. Так, за весь 2019 год в результате 25 утечек, что втрое превышает количество случаев за 2018 г., на черном рынке оказалось 2,2 млн записей — персональных данных клиентов и коммерческих секретов организаций. Несмотря на то, что общемировые темпы роста числа утечек, гораздо ниже, за 2019 год аналитики InfoWatch насчитали 158 случаев утечек персональных данных в мире, что на 42% превышает показатели предыдущего года [6]. Особую угрозу в данном случае представляет расширение масштабов утечки персональных данных. По итогам 2018 г. в результате хакерских атак непреднамеренно были раскрыты персональные данные пользователей 4800 сайтами, в результате чего было скомпрометировано 563 млн. учетных записей [7].

В данном случае достаточно важно отметить, что наибольший вес данных, подвергшихся утечке, приходился далеко не на банковскую сферу. По итогам 2019 г. 82% всех украденных записей пришлось на транспортную сферу. Утечки данных в таких компаниях имеют достаточно большие объемы: в среднем 1,15 млн. записей за один инцидент, 75% из которых представляют персональные данные клиентов [10].

В последнее время информационные системы аэропортов всё чаще подвергаются кибератакам, в результате чего происходит утечка баз данных, в частности персональных. Один из последних таких инцидентов произошел в Оренбургской области. В сеть выложили списки с личными данными 270 пассажиров самолета, прибывшего из Таиланда, а именно: ФИО, даты рождения, адреса и телефоны бывших туристов.

Компании авиационной отрасли, по оценкам экспертов, попадают в число тех предприятий, которым требуется максимальная защищенность в силу оперирования ими следующими сведениями:

– персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья и интимной жизни (категория 1);

– персональные данные, позволяющие идентифицировать пользователя и получить о нем необходимую информацию, в том числе относящуюся к категории один (категория 2).

В 2019 году эксперты компании ImmuniWeb изучили кибербезопасность 100 лучших аэропортов мира из шести глобальных регионов, отобранных компанией Skytrax для участия в конкурсе World Airport Awards, в их числе были такие отечественные аэропорты как:

– Московский международный аэропорт «Домодедово»;

– Московский международный аэропорт «Шереметьево» (рисунок 5).

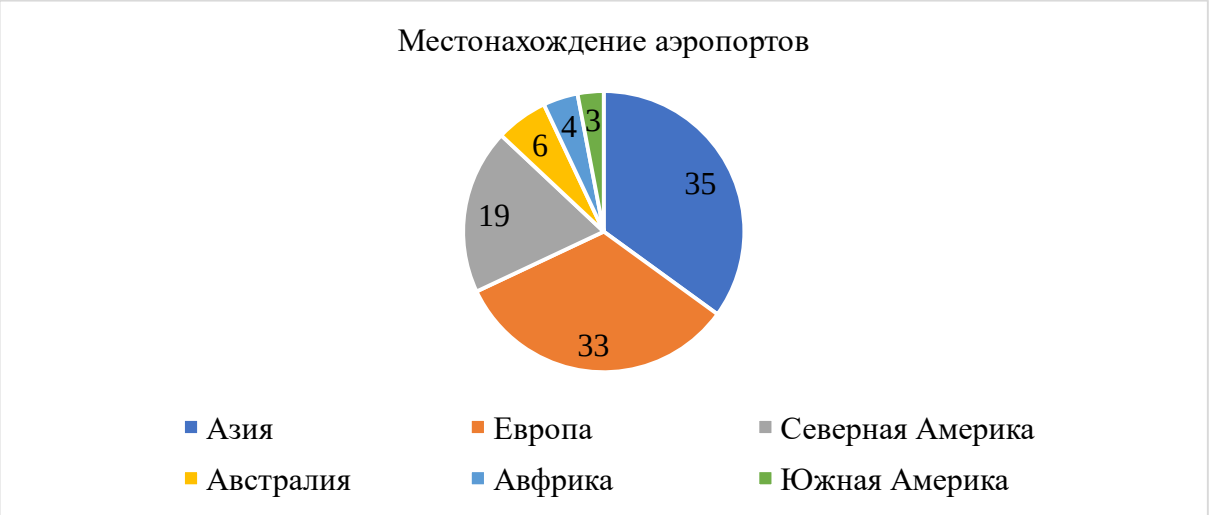


Рисунок 5. Расположение по континентам изученных аэропортов

Источник: составлено авторами по данным [11]

Эксперты ImmuniWeb при проверке системы безопасности аэропортов тестировали их публичные сайты и официальные мобильные приложения, а также проводили поиск утечек данных через облачные сервисы, публичные репозитории и DarkNet. В частности, экспертами были проверены:

– корректность реализации HTTPS;

– поддержка почтовым сервером аэропорта SPF, DKIM и DMARC;

– обновление CMS сайта до последних версий и уязвимость компонентов;

– соответствие стандартам PCI DSS, NIST и HIPAA;

– наличие WAF в системах аэропорта;

– настройки cookie, header и т. д.;

– мобильные приложения компонентов на уязвимость для известных эксплоитов;

– связь мобильных приложений со сторонними библиотеками и фреймворками;

– базовые настройки безопасности мобильных приложений;

– доступность данных, связанных с аэропортом, в публичных облачных сервисах хранения данных, репозиториях, DarkNet, хакерских сайтах.

По результатам анализа сайтов и мобильных приложений были выявлены следующие проблемы:

– 97% сайтов работают с устаревшим ПО;

– 24% сайтов содержат известные и эксплуатируемые уязвимости;

– 76% и 73% сайтов не соответствуют GDPR и PCI DSS соответственно;

– 24% сайтов не имеют SSL-шифрования или используют устаревший SSLv3;

– 55% сайтов защищены WAF;

– 100% мобильных приложений содержат как минимум 5 внешних программных фреймворков;

– 100% мобильных приложений содержат как минимум 2 уязвимости;

– в среднем в каждом приложении обнаруживается 15 проблем безопасности или конфиденциальности;

– 33,7% исходящего трафика мобильных приложений не имеют шифрования;

– данные 66% аэропортов можно найти в DarkNet;

– 87% аэропортов имеют утечки данных в общедоступных репозиториях;

– 503 из 3184 утечек имеют критический или высокий риск, который потенциально может привести к взлому;

– 3% аэропортов работают с незащищенным публичным облаком с конфиденциальными данными.

Таким образом, при проверке было выявлено, что 97% аэропортов имеют те или иные проблемы с кибербезопасностью, а слабые места приложений и уязвимости программного обеспечения по-прежнему остаются наиболее распространенными средствами, с помощью которых киберпреступники осуществляют внешние атаки.

Исходя из вышесказанного, становится очевидным, что защита собранных персональных данных как сотрудников, так и пассажиров, является ключевым звеном в обеспечении информационной безопасности аэропортов.

В таблице 1 представлены сведения о политике обработки персональных данных (ПД) отечественных аэропортов.

Таблица 1

Способы защиты персональных данных пассажиров Российских аэропортов

| Наименование аэропорта | Наличие политики обработки ПД | Признание аэропорта как оператора ПД | Наличие мероприятий по защите ПД |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| АО «Международный аэропорт «Внуково» | + (определяет основные принципы, цели, условия и способы обработки, требования к защите ПД) | + | + (устанавливаются в соответствии с локальными нормативными актами, регламентирующими вопросы обеспечения безопасности ПД при их обработке в информационных системах) |
| АО «Международный аэропорт «Калуга» | + (определяет порядок и условия обработки персональных данных) | + | + (принимаются правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и др. несанкционированных действий) |
| АО «Международный аэропорт Шереметьево» | + (определяет порядок и условия обработки ПД) | + | + (обеспечиваются раздельное хранение ПД, сохранность, технические мероприятия по исключению несанкционированного доступа, резервное копирование данных, постоянный контроль за обеспечением уровня защищенности ПД) |
| ПАО «Аэропорт Кольцово» | + (определяет порядок и условия обработки ПД) | - (обработка ПД осуществляется специализированными организациями) | + (после обработки ПД помещаются в архив, затем уничтожаются по истечению соответствующего срока хранения. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность) |

Продолжение таблицы 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| АО «Аэропорт Рощино» | + (определяет порядок и условия обработки ПД) | + | + (принимаются необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий) |

Источник: составлено авторами на основе данных [12-16]

Из представленных данных видно, что не все аэропорты признаются операторами персональных данных пассажиров, но, несмотря на это, осуществляют обработку данных и проводят практически идентичные мероприятия, направленные на их защиту.

Наличие политики обработки персональных данных, а также установление ряда обязательных мероприятий по их защите, безусловно, позволяют минимизировать угрозы утечки персональных данных, но не исключают их. Несмотря на достаточно высокий уровень угрозы, сбор сведений о пассажирах является необходимым элементом деятельности любого аэропорта. Дело в том, что аэропорты формируют и ведут базы данных, которые необходимы для авиалогистики, в то время как паспортные данные и иные персональные данные пассажиров - для дальнейшей их идентификации при регистрации на рейс (рисунок 6).

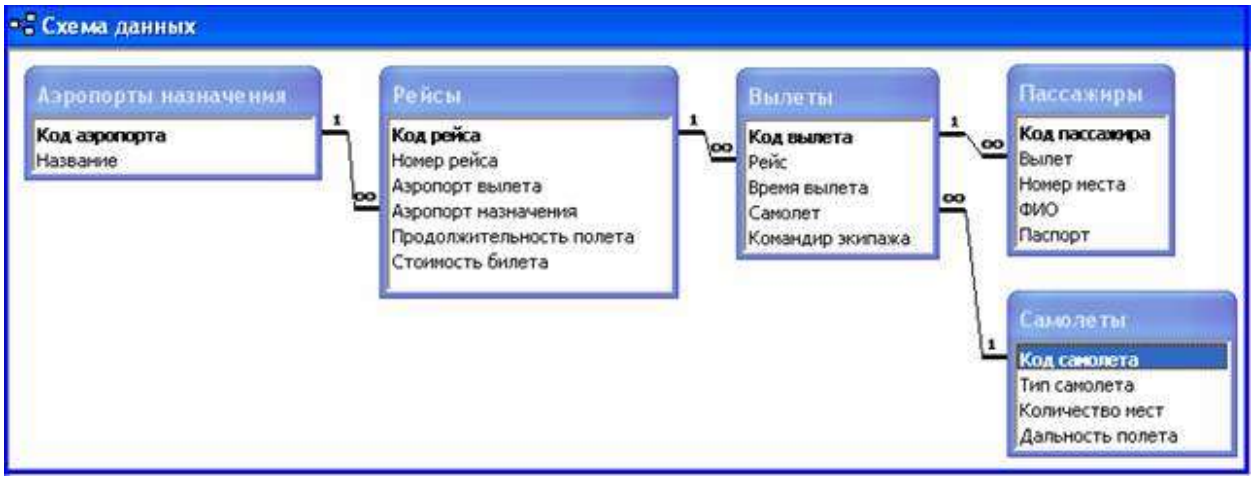


Рисунок 6. Схема взаимосвязи баз данных, формируемых аэропортами, и персональных данных пассажиров

Источник: [17]

Помимо этого, стоит также отметить, что с ростом цифровизации экономики многие аэропорты, помимо привычных персональных данных (паспортных, ФИО и номеров телефонов), начали сбор и обработку биометрических данных пассажиров. Для ускорения процессов регистрации пассажиров на рейсы и прохождения паспортного контроля аэропорты реализуют концепцию «лицо, как паспорт», что позволяет повысить их пропускную способность.

Особенно активно данное направление развивается в зарубежных странах. Так, управление таможенной и пограничной охраны США тестирует биометрию для выхода на посадку в 15 главных аэропортах страны, а аэропорты в Риме, Болонье и Неаполе уже внедрили биометрический паспортный контроль. В России же только делаются первые шаги по использованию биометрической идентификации пассажиров в силу консервативности нормативной базы, тормозящей развитие использования пассажирской биометрии. Тем не менее, для обеспечения контроля внутренней безопасности технологии биометрии уже достаточно широко используются в российских аэропортах.

Таким образом, с приходом цифровизации экономики увеличивается не только объём собираемой информации в части персональных данных, но и угрозы, побуждающие операторов персональных данных совершенствовать систему их защиты с целью предотвращения утечек и обеспечения безопасности.

**Библиографический список**

1. О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 06.04.2021).

2. Актуальные киберугрозы: II квартал 2020 года // Positive Technologies: [сайт]. [дата публ. 26.08.2020]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/ (дата обращения: 06.04.2021).

3. Топ-5 глобальных рисков в 2019 году по мнению Всемирного экономического форума // BCS EXPRESS: [сайт]. [дата публ. 22.01.2019]. URL: https://bcs-express.ru/novosti-i-analitika/top-5-global-nykh-riskov-v-2019-godu-po-mneniiu-vsemirnogo-ekonomicheskogo-foruma (дата обращения: 06.04.2021).

4. Утечки данных из банков России // TADVISER: [сайт]. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России (дата обращения: 06.04.2021).

5. Статистика и факты кражи личных данных: 2018 – 2019 // HERITAGE-OFFSHORE: [сайт]. URL: https://heritage-offshore.com/zashhita-ot-krazhi-lichnyh-dannyh/statistika-i-fakty-krazhi-lichnyh-dannyh-2018-2019/ (дата обращения: 06.04.2021).

6. Виды мошенничества с паспортными данными // Юридическая помощь онлайн 24/7: [сайт]. [дата публ. январь 2020]. URL: https://prolaw24.ru/criminal/moshennichestvo-s-pasportnymi-dannymi (дата обращения: 06.04.2021).

7. Российская банковская система сегодня: взаимодействие реального и финансового секторов в условиях цифровизации экономики // Ассоциация банков России: [информационно-аналитическое обозрение]. [дата публ. сентябрь 2020]. URL: https://asros.ru/upload/iblock/c30/20397_informatsionnoanaliticheskoeobozreniesentyabr2019.pdf (дата обращения: 06.04.2021).

8. Сбербанк: социальная инженерия используется в 9 из 10 случаев кибератак на банки // BLOOM CHAIN: [сайт]. [дата публ. 19.06.2020]. URL: https://bloomchain.ru/newsfeed/sberbank-socialnaja-inzhenerija-ispolzuetsja-v-9-iz-10-sluchaev-kiberatak-na-banki (дата обращения: 06.04.2021).

9. Клерки подвели клиентов: как воруют банковские данные // ГАЗЕТА.RU: [сайт]. [дата публ. 06.11.2019]. URL: https://www.gazeta.ru/business/2019/11/06/12797714.shtml (дата обращения: 06.04.2021).

10. Персональная безответственность: количество утечек данных в России выросло в 10 раз // Известия: [сайт]. [дата публ. 29.10.2020]. URL: https://iz.ru/1079257/anastasiia-gavriliuk/personalnaia-bezotvetstvennost-kolichestvo-utechek-dannykh-v-rossii-vyroslo-v-10-raz (дата обращения: 06.04.2021).

11. State of Cybersecurity at Top 100 Global Airports // ImmuniWeb SA Application Security Series: [сайт]. [дата публ. 29.01.2020]. URL: https://www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html (дата обращения: 06.04.2021).

12. Политика АО «Аэропорт Рощино» в отношении обработки персональных данных // Международный аэропорт Тюмень Рощино: [официальный сайт]. URL: https://tjm.aero/airport/privat_info/ (дата обращения: 06.04.2021).

13. Политика в отношении обработки персональных данных // Международный аэропорт Калуга имени К. Э. Циолковского: [официальный сайт]. [дата публ. 06.03.2020]. URL: https://klf.aero/airport/policy-on-the-processing-of-personal-data/ (дата обращения: 06.04.2021).

14. Политика обеспечения безопасности персональных данных // Кольцово Международный Аэропорт Екатеринбурга: [официальный сайт]. [дата публ. 06.03.2020]. URL: http://svx.aero/privacy/ (дата обращения: 06.04.2021).

15. Политика обработки персональных данных // Внуково Международный аэропорт: [официальный сайт]. [дата публ. 22.02.2017]. URL: http://corp.vnukovo.ru/general-information/privacy-policy/ (дата обращения: 06.04.2021).

16. Политика обработки персональных данных // Шереметьево Международный аэропорт: [официальный сайт]. [дата публ. 01.04.2019]. URL: https://www.svo.aero/ru/passengers/airport-rules/privacy (дата обращения: 06.04.2021).

17. База данных Аэропорт // Access: Базы данных и СУБД [сайт]. URL: http://bd-subd.ru/access/baza-dannih-aeroport.htm (дата обращения: 06.04.2021).