УДК 314.02; 004.056

ГРИГОРЬЕВ ОЛЕГ МИХАЙЛОВИЧ,
МАТВЕЕВ ВЛАДИМИР ВЛАДИМИРОВИЧ

АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИССЛЕДОВАНИИ ДЕМОГРАФИЧЕСКИХ ПРОЦЕССОВ

АННОТАЦИЯ

Рассмотрено исследование демографических процессов с позиции информационной безопасности. Приведены основные угрозы информационной безопасности источников демографической информации. Описаны основные критерии и алгоритм построения комплексной системы обеспечения информационной безопасности. Рассмотрены основы методологического аппарата информационной безопасности в демографических исследованиях.

Ключевые слова: информационная безопасность; демография; угрозы информации; перепись населения; комплексная система защиты информации; системный подход; криптография; электронная подпись.

GRIGOREV O.M.,
MATVEEV V.V.

ASPECT OF INFORMATION SECURITY IN THE DEMOGRAPCHIC PROCESSES RESEARCH

ABSTRACT

The research of demographic processes from the position of information security is considered. The main information security threats for demographic information sources are shown. The main criteria and algorithm for constructing an integrated information security system are described. The fundamentals of the methodological apparatus of information security in demographic research are shown.

Keywords: information security; demography; information threats; population census; comprehensive information security system; system approach; cryptography; electronic signature.

Информация о населении, используемая в демографических исследованиях, является общедоступной и не подлежит отнесению к государственной тайне и засекречиванию согласно закону РФ «О государственной тайне» [1]. Демографическая информация формируется из двух основных источников: переписи населения и текущего учета естественного и миграционного движения.

Особенность переписи населения заключается в том, что только она позволяет получить информацию о численности и возрастной структуре населения во всех, даже самых мелких территориальных единицах. Для определения некоторых переменных (фактический брачный статус, язык, образовательная структура населения, национальность) перепись незаменима.

С другой стороны, получаемые в ходе переписи населения данные можно лишь условно считать достоверными, т.к. проверить честность респондента в большинстве ответов не представляется возможным. Таким образом, можно сделать вывод, что даже на стадии сбора необходимой для демографического исследования информации есть вероятность её искажения, способного повлиять на результаты всей работы.

Следующим уязвимым местом информации

в демографии является её обработка и предоставление конечному пользователю. В ходе данного процесса возможна как подмена данных (например, для сокрытия плохих показателей работы местных органов государственной власти), так и их искажение вследствие некорректной работы программных средств, т.е. тем самым нарушается безопасность информации [2].

Следует отметить, что деструктивному воздействию также могут быть подвержены носители демографической информации и информационные ресурсы, на которых она располагается. Эти действия могут привести к полной утрате, искажению или недоступности данных.

Данные, получаемые в ходе демографических исследований, являются основой для принятия управленческих решений на всех уровнях государственного управления и содержат много сопутствующей информации, не подлежащей разглашению (например, персональные данные). В связи с этим нужно говорить о важности обеспечения информационной безопасности при проведении демографических исследований и сбора демографических показателей.

Защита демографической информации подразумевает совокупность мероприятий, направленных на обеспечение целостности обрабатываемой информации (данные не были изменены при передаче, хранении и отображении), а также доступности информации для пользователей (обеспечение беспрепятственного и своевременного доступа пользователей к информации) [3]. В связи с тем, что демографическая информация хранится длительное время, она должна подлежать постоянной защите, ее уничтожение осуществляется по определенным командам [4, с.55].

Безопасность связана с защитой демографической информации от угроз. Во внимание следует принимать все разновидности угроз, но в сфере безопасности демографической информации наибольшее внимание уделяется тем из них, которые связаны со злонамеренными или иными действиями человека [5].

В связи с этим можно считать, что безопасность информационных демографических систем – это защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного и искусственного характера, которые могут нарушить доступность, целостность и конфиденциальность информации [6, с.33].

Управление информационной безопасностью в демографии – циклический процесс, состоящий из совокупности целенаправленных действий, осуществляемых для достижения заявленных целей посредством обеспечения защищенности информационной сферы, и включающий осознание необходимости обеспечения информационной безопасности источника демографической информации, постановку задачи по ее обеспечению, оценку текущей ситуации, планирование мер по обработке рисков информационной безопасности, реализацию, внедрение и оценку эффективности соответствующих защитных мероприятий и средств управления, распределение ролей и ответственности в области информационной безопасности, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию [7, с.135-136]. Стоит отметить, что необходимо обеспечивать защиту не только хранящейся демографической информации, но и информации, которая передается по каналам связи или обрабатывается программным обеспечением.

Для обеспечения достоверности и целостности демографической информации в государственных информационных системах [8] необходимо наличие определенных видов обеспечения: нормативно-правового, организационно-технического, программного и аппаратного.

Угрозы для демографической информации в общем виде выражаются в нарушении ее целостности (искажение, ошибки, потери) и доступности (нарушение связи). Нарушителя следует описывать через такие аспекты, как компетентность, доступные ресурсы и мотивация. Нападение следует описывать через такие аспекты, как возможность, метод нападения и используемые уязвимости [5].

С другой стороны, угрозы для демографической информации представляется возможным разделить по трем компонентам государственной информационной системы и ее инфраструктуры, на которые непосредственно направлена данная угроза. В этом случае классификация выглядит следующим образом: угрозы информации, угрозы программному обеспечению информационной системы, угрозы системному программному обеспечению, угрозы

компьютерной технике и сетевому оборудованию. Следует разделять случайные (возникают независимо от воли людей) и преднамеренные (всегда создаются намеренными действиями людей) [6, с.34].

Классификацию угроз информационной безопасности в демографии можно также представить в следующем виде:

– происшествия, связанные с техническими причинами (сбой технических систем, отказ ПО, ошибки при передаче данных, потеря данных на носителе, воздействие вредоносных программ);
– происшествия, связанные со стихийными бедствиями (пожар, затопление);
– происшествия, связанные с ненамеренными действиями людей (ошибки оператора, администратора, порча оборудования или носителей информации, отсутствие надлежащего технического обслуживания);
– злоумышленные действия людей (диверсия, компрометация ключей доступа, заражение системы вредоносными программами, блокировка каналов связи или работы системы, повреждение или удаление информации) [9, с.115-119].

В общем виде можно говорить о трех видах угроз: угрозы доступности демографической информации, угрозы целостности демографической информации и угрозы конфиденциальности демографической информации. В связи с тем, что демографическая информация является открытой, последние угрозы рассматриваться не будут.

Угрозы доступности и целостности демографической информации обычно схожи и бывают вызваны аналогичными причинами.

В первую очередь следует обратить внимание на отказ со стороны пользователей государственной информационной системы. К этой группе можно отнести непреднамеренные ошибки, нежелание работать с информационной системой вследствие отсутствия необходимых знаний и невозможность работы с системой из-за отсутствия необходимой документации или допуска.

Второй группой причин возникновения угроз является внутренний отказ государственной информационной системы. Включает в себя выход системы из штатного режима эксплуатации, ошибки конфигурирования системы, разрушение данных.

Третья группа – внешние источники возможного нарушения доступа к данным: нарушение условий работы; отказ, повреждение или разрушение аппаратных средств; разрушение или повреждение помещений; сетевые и вирусные атаки; разрушение информации действиями человека [6, с.35-37].

Последствиями проведения информационных атак на источники демографической информации могут стать искажение информации, навязывание ложной информации, нарушение установленного порядка сбора, обработки и передачи информации, отказы и сбои в работе технических систем. Количество правонарушений в данной области увеличивается в связи с повсеместным внедрением автоматизированной обработки информации. В связи с этим на ведущие роли выходит надежное обеспечение сохранности информации, циркулирующей и обрабатываемой в государственных информационных системах и сетях.

В общем виде нарушения безопасности источника демографической информации возникают вследствие преднамеренного использования или непреднамеренной активации уязвимостей при применении информационной системы по назначению. Уязвимости могут возникать из-за недостатков:

– требований, т.е. информационная система может обладать требуемыми от неё функциями и свойствами, но все же содержать уязвимости, которые делают ее непригодной или неэффективной в части безопасности;
– проектирования, т.е. информационная система не отвечает спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;
– эксплуатации, т.е. информационная система разработана в полном соответствии с корректной спецификацией, но уязвимости возникают как результат неадекватного управления при эксплуатации [5].

Основными мерами защиты доступности демографической информации являются:

– корректная организация труда;
– адекватный подбор кадров и необходимая подготовка сотрудников;
– качественная разработка и конфигурирование системы;

- максимально возможное тестирование информационной системы;
- резервное копирование данных;
- наличие средств защиты каналов связи;
- наличие резервного оборудования и помещений;
- наличие в системе протоколирования (фиксации всех действий пользователей);
- аудит (анализ накопленных данных по активности пользователей);
- межсетевое экранирование (фильтрация потоков между двумя сетями) [6, с.37-38].

Если речь идет о защите целостности демографической информации, следует добавить механизмы оперативного восстановления утраченной информации, контроль ввода данных и тестирование системы на предмет нарушения целостности с быстрым реагированием на выявленные нарушения [6, с.37-38].

Комплексный (системный) подход к построению системы защиты демографической информации включает в себя: прежде всего, изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми необходимо оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца [10].

Обеспечение информационной безопасности в демографии может достигаться системой мер, состоящей из следующих элементов:

- предупреждение угроз;
- выявление угроз;
- обнаружение угроз;
- локализация преступных действий;
- ликвидация последствий.

Существенную роль в данной системе играет информационно-аналитическая деятельность. Для обеспечения достаточного уровня информационной безопасности источников демографической информации необходимы ориентация на упреждающий характер действий и проведение заблаговременных мер предупреждения возможных угроз.

На сложность системы информационной безопасности источника демографической информации влияет степень автоматизации процедур обработки информации. В государственной информационной системе может быть реализована автоматизация процесса подготовки документов (учет, контроль, базы данных, электронные архивы); автоматизация документооборота (электронный документооборот), позволяющая обмениваться документами как между структурными подразделениями, так и с внешними объектами (отчетность в контролирующие органы); использование автоматизированных систем управления производственными процессами. Для обеспечения безопасности используются криптографические средства, электронные подписи, защищенные каналы связи.

Одной из основных проблем реализации системы защиты демографической информации является:

- с одной стороны, обеспечение надежной защиты находящейся в системе информации, исключение случайного или преднамеренного получения доступа к системе посторонними лицами, разграничение доступа к ресурсам;
- с другой стороны, системы защиты не должны создавать заметных неудобств пользователям в процессе работы с системой.

Поэтому основной задачей системы информационной безопасности в демографии является аутентификация пользователя. Это позволяет как лишить доступа к системе лиц, не имеющих на это право, так и ограничить круг пользователей, которые могут внести изменения или удалить информацию. В настоящее время одним из наиболее распространенных и удобных средств аутентификации является электронная подпись [11]. Дополнительной мерой защиты информации является разграничение прав пользователей [4, с.34].

Для источника демографической информации должна применяться утвержденная руководством политика информационной безопасности, которая должна содержать:

- определение информационной безопасности в терминах деятельности данной информационной системы, области действия политики, целей, задач и принципов информационной безопасности;
- общие сведения об активах, подлежащих защите, и их классификацию;

– модели угроз и нарушителей информационной безопасности;
– санкции и последствия нарушений политики;
– определение общих ролей и обязанностей, связанных с информационной безопасностью [7, с.103].

Важной составляющей системы информационной безопасности в демографии является комплекс мер по защите от сетевых атак, вирусных и других вредоносных программ. Построение указанного комплекса осуществляется с использованием трех рубежей защиты:

1. Защита от проникновения в систему вредоносных программ.
2. Своевременное обнаружение проникновения вируса и его ликвидация.
3. Ликвидация последствий проникновения в систему вредоносных программ или сетевой атаки [6, с.37-38].

Целью защиты информации в области демографии должно быть обеспечение достоверности информации, защиты от навязывания ложной информации, ее своевременного предоставления. Как и в большинстве профессиональных областей, только системный подход к организации информационной безопасности может обеспечить достижение поставленных целей.

Вышеуказанные факторы свидетельствуют о необходимости применения комплексной системы защиты информации, используемой для проведения демографических исследований. Обеспечение безопасности демографической информации не может быть одноразовым актом. Это непрерывный процесс, включающий обоснование и реализацию наиболее рациональных методов совершенствования и развития системы защиты, постоянный контроль её состояния, выявление её слабых мест и возможных противоправных действий. Уровень защищенности любой информационной системы соответствует защищенности ее самого слабого звена. Безопасность демографической информации может быть обеспечена лишь при комплексном использовании имеющихся средств защиты во всех структурных элементах и на всех этапах технологического цикла обработки информации.

При проектировании системы безопасности демографической информации следует в первую очередь принять меры по уменьшению количества потенциальных уязвимостей, возможностей их проявления, а также минимизации степени ущерба при проявлении уязвимости.

Список литературы

1. Закон РФ «О государственной тайне» от 21.07.1993 г. №5485-I (в ред. от 26.07.2017 г.).
2. Положение о государственном лицензировании деятельности в области защиты информации (утв. решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации №10 от 27 апреля 1994 г. и №60 от 24 июня 1997 г.).
3. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
4. *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Технические, организационные и к адровые аспекты управления информационной безопасностью. – М.: Горячая линия – Телеком, 2012. – 214 с.
5. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
6. *Пирогов В.Ю.* Информационные системы и базы данных: организация и проектирование. – СПб.: БХВ-Петербург, 2009. – 528 с.
7. *Курило А.П.* [и др.] Основы управления информационной безопасностью. – М.: Горячая линия – Телеком. – 2014. – 244 с.
8. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ (в ред. от 31.12.2017 г.)
9. *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Управление рисками информационной безопасности. – М.: Горячая линия – Телеком, 2014. – 130 с.
10. *Галатенко В.А.* Основы информационной безопасности. – М.: Интуит.Ру, 2005.
11. Федеральный закон «Об электронной подписи» от 06.04.2011 №63-ФЗ (ред. от 23.06.2016 г.).

Статья поступила в редакцию 14 сентября 2018 г.
Принята к публикации 23 ноября 2018 г.