Чвала Д.А. Основные источники угроз в информационных системах персональных данных // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 57–61

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ОСНОВНЫЕ ИСТОЧНИКИ УГРОЗ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Чвала Д.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: chvala_d@mail.ru

В данной статье обозреваются основные источники угроз безопасности персональных данных. В повседневной жизни человека безопасность информации о его жизни зависит от него самого. Но ситуация совершенно иная, когда мы обязаны предоставлять данные о нас третьим лицам, в частности работодателю, в соответствии с законом. В этой ситуации сотрудник передает конфиденциальную информацию о себе для хранения. Кроме того, работодатель уже отвечает за безопасность данных. Он обязан защищать информацию о сотрудниках от посягательств третьих лиц и несет ответственность за передачу этих данных. Возрастающая сложность методов и средств организации машинной обработки, широкое использование глобальной сети Интернета приводят к тому, что информация становится все более уязвимой

Ключевые слова: Угрозы, безопасность, персональные данные, классификация угроз.

MAIN SOURCES OF THREATS IN PERSONAL DATA INFORMATION SYSTEMS

Chvala D.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: chvala_d@mail.ru

This article reviews the main sources of threats to the security of personal data. In a person's daily life, the security of information about his life depends on him. But the situation is completely different when we are obliged to provide data about us to third parties, in particular to the employer, in accordance with the law. In this situation, the employee transfers confidential information about himself for storage. In addition, the employer is already responsible for data security. He is obliged to protect information about employees from the encroachments of third parties and is responsible for the transfer of this data. The increasing complexity of methods and means of organizing machine processing, the widespread use of the global Internet network lead to the fact that information is becoming more vulnerable

Keywords: Threats, security, personal data, classification of threats.

Введение

Сначала стоит вспомнить само понятие о персональных данных:

- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
- Информация может храниться в разных видах:
- Устная;

- Визуальная;
- Цифровая форма.

Информация в устном виде передается по акустическим путям: аудио воспроизведение, речь и т.д. Визуальная – отображение на каких-либо физических носителях: печатные документы, отображение на экранах девайсов и т.д., и, наконец, цифровая – информация, располагающаяся на цифровых носителях, хранящаяся в системах информационной среды и прочее. [1]

К разной информации есть разные варианты несанкционированного доступа, которые может использовать нарушитель. Все зависит от уровня его доступа к системе, которая стала его целью. Также это может зависеть от таких факторов, как неаккуратность работающего персонала в компании, которая причастна к работе системы хранения персональных данных, или от имеющихся методов несанкционированного доступа у нарушителя, либо произошедший случай инцидента был случайным и лицо, ставшее нарушителем, не имело целей прийти к таким результатам.

Общая характеристика источников угроз в информационных системах персональных данных.

НСД может быть реализован в ИСПД с использованием программного и аппаратного обеспечения, если осуществление несанкционированного, в том числе случайного, доступа, которое нарушает конфиденциальность, целостность и доступность ПДн, и включает в себя:

- угрозы несанкционированного доступа к операционной среде компьютера со стандартным программным обеспечением (инструменты операционной системы или общие прикладные программы);
- угрозы создания нестандартных режимов работы программных (программных) средств путем преднамеренного изменения официальных данных, игнорирования ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных. [2]

Кроме того, возможны комбинированные угрозы, которые представляют собой комбинацию этих угроз. Например, внедрение вредоносного ПО может создать условия для NRD в операционной среде компьютера, в том числе путем формирования нетрадиционных информационных каналов для доступа. Угрозы несанкционированного доступа к операционной среде программного обеспечения по умолчанию делятся на прямые и удаленные угрозы. Прямой доступ осуществляется через программный и аппаратный ввод-вывод компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевой связи. Такие угрозы угрожают ISPD как на основе рабочего места, которое не является членом общедоступной сети связи, так и на всех интернет-провайдерах, которые подключаются к сетям связи и международным сетям для обмена информацией.

Классификация угроз информационной безопасности персональных данных.

Под угрозой информационной безопасности понимается угроза нарушения свойств информационной безопасности – доступности, целостности или конфиденциальности информационных активов организации. Перечень угроз, оценка вероятности их реализации, а также модель злоумышленника составляют основу для анализа риска угроз и формулировки требований по защите автоматизированной системы. Помимо выявления возможных угроз,

необходимо проанализировать выявленные угрозы на основе их классификации по ряду признаков. Угрозы, соответствующие каждому признаку классификации, позволяют вам подробно изложить требования, отраженные в этом признаке. Поскольку информация, которая хранится и обрабатывается в современных автоматизированных системах управления, подвергается воздействию чрезвычайно большого количества факторов, формализовать задачу и описать полный набор угроз становится невозможным. Чтобы поделить нарушителей на категории, надо проанализировать их отношение к системе персональных: человек может быть либо сотрудником организации, имеющей доступ к системе персональных данных, либо может быть не связан с ней, но иметь цель получить несанкционированный доступ к данным.

Отсюда можно поделить нарушителей на две категории:[3]

- 1 категория: лица, имеющие доступ в информационной системе персональных данных;
- 2 категория: лица, не имеющие доступ к информационной системе персональных данных.

Еще одна категория, на которую можно разделить нарушителей, это категория относительно местоположения: внутри или вне контролируемой зоны.

Отсюда еще две группы: внешние нарушители и внутренние нарушители.

Несмотря на две последние группы, 1 категория нарушителей имеет как внутренних нарушителей, так и внешних. Последними могут быть те же лица из внутренней категории, находящиеся за территорией контролируемой зоны. Такие лица имеют достаточное количество знаний об информационной системе персональных данных для совершения атаки или создания инцидента.[4]

Нормативно-правовое регулирование.

Федеральный закон «О персональных данных» предусматривает, что данные граждан, их личная жизнь, имущественный статус и состояние здоровья, хранимые и обработанные в информационных системах, не может быть неправомерно передано третьим лицам. Несовершенство системы обработки информации нередко приводит к утечке важных данных, включая персональные данные. Утечка может быть случайной или преднамеренной. Для того, чтобы избежать подобных ситуаций, которые могут причинить вред гражданам, разработаны специальные стандарты для информационных систем. Для организации, признанной в соответствии с законом оператором персональной информации, технические требования к системам обработки данных устанавливаются приказами ФСТЭК РФ. В настоящее время действует распоряжение №21, вступившее в силу 2013 года, которое определяет технические, организационные и технические мероприятия по обеспечению защиты персональной информации. Оно неоднократно было дополнено и изменено в зависимости от требований времени. В структуре документа в приложении о составе мер содержатся рекомендация о регулировании:

- Идентификацию и аттестацию лиц, допускаемых операторами к обработке данных;
- Управление доступом к ним;
- Программную среду и ограничения;
- Физическую защиту компьютеров, в которых содержатся данные, связанные с персональной информацией;
- Правила регистрации происшествий безопасности;

- Правила организации антивирусных защит;
- Правила фиксации попадания в защищенные информационные периметры;
- Отслеживание защищенности личных данных;
- Защита технического обеспечения.

Выбор мер технической и организационной защиты личных данных будет зависеть от класса защиты информационных систем, определённого по правилам, предусмотренными постановлением Правительства №1119.[5]

Заключение.

В заключение можно отметить, что защита персональных данных в информационных системах является одной из ключевых задач современной кибербезопасности. Множество угроз, таких как несанкционированный доступ к операционной среде, преднамеренное искажение данных или внедрение вредоносного программного обеспечения, требуют комплексного подхода к обеспечению безопасности. Важно не только выявлять потенциальные угрозы, но и классифицировать их для разработки эффективных мер защиты. Федеральные нормативно-правовые акты, такие как закон «О персональных данных» и распоряжения ФСТЭК, играют важную роль в создании четких требований к защите данных. Комплекс мер, включающий управление доступом, контроль за информационными потоками, защиту физической и программной среды, должен применяться с учетом специфики информационной системы и степени угроз, что позволит минимизировать риски и обеспечить надежную защиту персональных данных.

Список литературы

1. Цветков, А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux/А.Ю.Цветков//Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662
2. Исследование существующих механизмов защиты операционных систем семейства Linux / А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662.
3. Багомедова А.Р., Ушаков И.А., Цветков А.Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник статей VII Международной научно-технической и научно-методической конференции. 2018. С. 58-63.
4. Катасонов А. И. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU Linux /А.И.Катасонов, С.И.Штеренберг, А.Ю.Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – No 2. – С. 50-56.
5. Захарова Т.Е., Цветков А.Ю. Анализ существующих нормативных документов для формирования политики безопасности в системе электронного документооборота

вуза//В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. СПб.: СПбГУТ, 2017. С. 337-343.

References

1. Tsvetkov, A.Yu. Research of existing mechanisms of protection of operating systems of the Linux family / A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VII International Scientific, Technical and scientific-methodological conference: collection of scientific articles in 4 volumes St. Petersburg: St. Petersburg State University, 2018. pp. 657-662
2. Investigation of the existing protection mechanisms of the operating systems of the family Linux / A.Y. Tsvetkov // Actual problems of infotelecommunications in science and education. VII International Scientific, Technical and scientific-methodological conference: collection of scientific articles in 4 volumes St. Petersburg: St. Petersburg State University, 2018. pp. 657-662.
3. Bagomedova A.R., Ushakov I.A., Tsvetkov A.Yu. Development of methods for verifying the compliance of virtualization servers with security requirements according to GOST R 56938-2016 standard // Actual problems of infotelecommunications in science and education (APINO 2018): collection of articles of the VII International Scientific, Technical and scientific-methodological Conference. 2018. pp. 58-63.
4. Katasonov, A. I. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in GNU Linux operating systems / A. I. Katasonov, S. I. Shterenberg, A. Yu. Tsvetkov // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 2. – pp. 50-56.
5. Zakharova T.E., Tsvetkov A.Y. Analysis of existing regulatory documents for the formation of a security policy in the electronic document management system university // In the collection: Current problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International Scientific , technical and scientific-methodical Conference. In 4 volumes. Edited by S.V. Bachevsky. St. Petersburg: St. Petersburg State University, 2017. pp. 337-343.