www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.1.4

УДК 004.056.5
ББК 32.972

АУДИТ СРЕДСТВ БЕЗОПАСНОСТИ ИСПДн

Александра Алексовна Даньшина

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
danshina1955a@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент,
кафедра информационной безопасности,
Волгоградский государственный университет
babenko.aleksey@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье предлагается модель проведения внешнего аудита программно-аппаратной части организации. Рассмотрены статистика утечки конфиденциальной информации за II квартал 2023 г., требования для информационной системы персональных данных, уровни защищенности информации и требования по защите ПДн. Представлены задачи, реализуемые предлагаемой моделью.

Ключевые слова: аудит средств безопасности, персональные данные, угроза, уровни защищенности, модель программного средства.

Информация является ценным ресурсом, а ее утрата может различным образом сказаться на репутации и доходах бизнеса. Именно поэтому проблема защиты персональных данных была и остается актуальной. По данным статистики [1] (см. рис. 1) за II квартал 2023 г. было выявлено следующее процентное соотношение утечки информации в организациях:

– 53 % ПДн;

– 18 % коммерческая тайна.

Для минимизации статистических данных о кибератаках и хищении персональных данных, а также сокращению числа угроз, вендоры, занимающиеся обеспечением информационной безопасности, с каждым годом предоставляют на рынок все более новые и усовершенствованные решения по обеспечению защиты ПДн.

На основе ФЗ № 307 компании, занимающиеся обработкой персональных данных и работой с информацией ограниченного доступа, должны проводить проверку нынешнего состояния защиты ИСПДн и удостоверяться, что применяемые аппаратные и программные средства актуальны и удовлетворяют всем нормам и требованиям. Для реализации данного мероприятия проводится аудит.

Аудит средств безопасности – это процесс систематической проверки и оценки средств и мер безопасности в информационной системе или организации. Целью такого аудита является выявление уязвимостей,

оценка эффективности существующих мер по защите информации, а также рекомендации по улучшению общей безопасности.

Данное мероприятие можно разделить на две категории:

1. Внутренний аудит проводится силами структурных подразделений компании и регламентируется документами организации.

2. Для проведения внешнего аудита организация заключает договор с экспертами и им организуется доступ к оцениваемой информации и инфраструктуре.

Разрабатываемый программный комплекс для проведения внешнего аудита информационной безопасности программно-аппаратной части организации должен выполнять следующие задачи:

1. Инвентаризация активов и классификация данных:

а) составление списка информационных активов, настройки групповой политики, базы данных и сети;

б) классификация персональных данных в соответствии с уровнем конфиденциальности.

2. Анализ конфигурации:

а) проверка настроек операционных систем, сетевых устройств и других программных и аппаратных компонентов на соответствие рекомендациям по безопасности.

3. Анализ политик и процедур безопасности:

а) проверка существующих политик безопасности и процедур в области обработки и защиты персональных данных;

б) оценка на соответствие требованиям НПА.

4. Управление доступом в организации к информационным ресурсам:

а) анализ системы управления доступом и аутентификации в организации;

б) мониторинг использования персональных данных и проверка прав доступа к ним.

5. Сканирование уязвимостей:

а) активное и пассивное сканирование сетевых устройств, ОС, приложений и других компонентов ИС с целью выявления известных уязвимостей.

6. Шифрование и защита данных:

а) оценка методов шифрования данных в покое и в движении;

б) анализ мер защиты данных на уровне хранения и передачи.

7. Мониторинг событий и обнаружение инцидентов:

а) проверка систем мониторинга безопасности и их способности обнаруживать инциденты, связанные с персональными данными;

б) оценка реакции на инциденты и процедур уведомления.

8. Тестирование на проникновение:

а) проведение тестирования на проникновение для выявления уязвимостей в системах обработки персональных данных;

б) эмуляция атак и попыток вторжения с целью проверки устойчивости системы к различным угрозам. Это может включать в себя тестирование наличия эксплойтов, брутфорс атаки, исследование возможных путей атаки и т. д.;

Рис. 1. Информация, которая интересует злоумышленников

в) оценка общей стойкости к внешним и внутренним угрозам.

9. Выявление и оценка степени уязвимости сетевых устройств:

а) проверка безопасности коммутаторов, маршрутизаторов и другого сетевого оборудования.

10. Проверка безопасности веб-приложений:

а) выявление уязвимостей веб-приложений, таких как SQL-инъекции, межсайтового скриптинга, переполнения буфера и др.

11. Составление отчетов и рекомендаций:

а) подготовка подробных отчетов об выявленных уязвимостях и рисках;

б) предоставление рекомендаций по улучшению безопасности.

Контекстная IDEF0-диаграмма аудита информационной безопасности разрабатываемого программного комплекса представлена на рисунке 2.

В функциональном блоке «Аудит информационной безопасности» заданы:

1. Входные данные – информационные активы, конфигурация баз данных, конфигурация сети, параметры групповой политики.

2. В качестве управляющей информации выступают требования НПА: ФСТЭК № 31, ГОСТ Р ИСО/МЭК ТО 15446-2008, ГОСТ Р ИСО/МЭК 15408-1-2012, ГОСТ Р ИСО/МЭК 27002–2012.

3. Средством для проведения аудита ИБ является разрабатываемый программный комплекс.

4. Результатом программы выступает выполнение требований по защите ИСПДн.

Декомпозиция функционального блока «Аудит информационной безопасности» представлена на рисунке 3.

Задачи программного комплекса можно изменять в соответствии с типом ИСПДн и уровнем защищенности информации. Опираясь на ПП РФ № 1119 и анализ исходных данных позволил определить УЗ данных в ИСПДн [2] (см. таблицу).

В данной таблице указаны уровни защищенности, которые можно описать следующим образом:

1. Уровень защищенности 4 (УЗ 4) – несекретная – информация, доступная для общественности без каких – либо ограничений. На данном уровне не предполагается конфиденциальность и ограничение доступа;

2. Уровень защищенности 3 (УЗ 3) – для служебного пользования – информация, предназначенная только для внутреннего использования внутри организации. Доступ для сторонних лиц ограничен.

3. Уровень защищенности 2 (УЗ 2) – секретная – информация, содержащая конфиденциальные данные, доступ к которым имеет ограниченный круг лиц, обладающий специальным разрешением.

4. Уровень защищенности 1 (УЗ 1) – совершенно секретно – информация, чья утрата или компрометация может представлять существенную угрозу для безопасности государства или организации.

Рис. 2. IDEF0-диаграмма аудита информационной безопасности

После анализа типа ИСПДн и уровня защищенности ПДн, программа может сформировать ряд требований [2] на основе ПП-1119:

1. Организация режима обеспечения безопасности помещений, где находится информационная система, направленного на предотвращение несанкционированного проникновения или нахождения в этих помещениях лиц без соответствующего права доступа.

2. Гарантирование целостности носителей персональных данных.

3. Наличие документа, утвержденного руководителем оператора, который определяет список лиц, имеющих доступ к обработке персональных данных в информационной системе, необходимый для выполнения ими своих служебных обязанностей.

4. Применение средств защиты информации, которые были подвергнуты процедуре проверки соответствия законодательству Российской Федерации в области обеспечения безопасности информации, при выявлении необходимости перекрытия текущих угроз.

5. Назначение сотрудника, отвечающего за обеспечение безопасности персональных данных в информационной системе обработки персональных данных.

6. Ограничение доступа к журналу электронных сообщений.

7. Запись в электронный журнал безопасности всех изменений в полномочиях сотрудника-оператора по доступу к персональным данным, хранящимся в информационной системе.

8. Учреждение структурного подразделения, обязанного обеспечивать безопасность

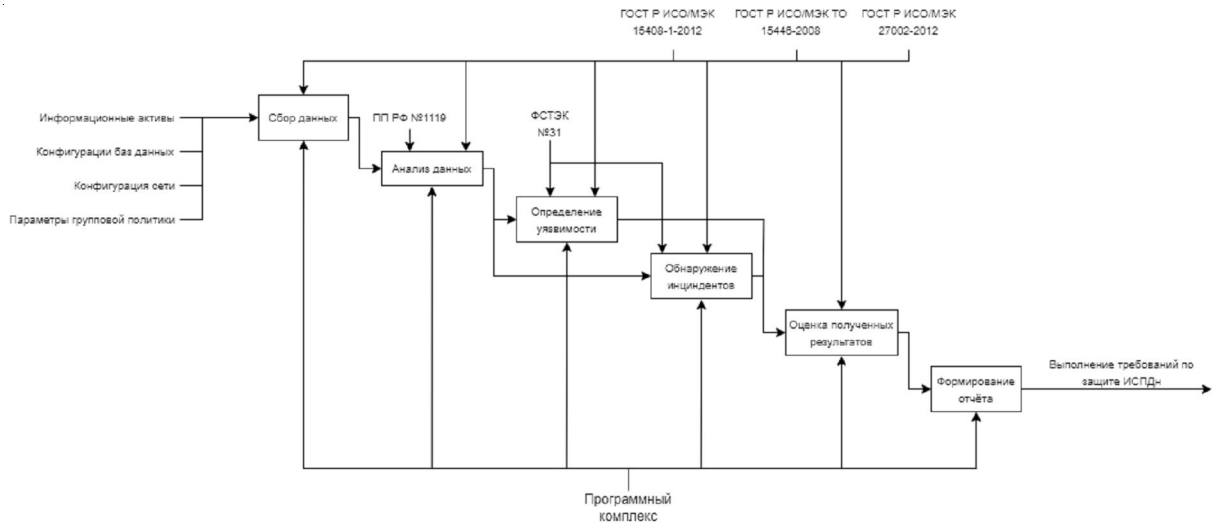

Рис. 3. Декомпозиция функционального блока «Аудит информационной безопасности»

Уровни защищенности ПДн

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1 (НДВ ОС)	2 (НДВ ПО)	3 (Без НДВ)
ИСПДн-С (специальные)	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б (биометрические)			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И (иные)	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О (общедоступные)	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4

персональных данных в информационной системе, или передача функций по обеспечению такой безопасности существующему структурному подразделению.

Представленный программный комплекс и предложенные им требования позволят минимизировать инциденты в компаниях, связанные с утечкой персональных данных или несанкционированными проникновениями. Перечень задач для программы аудита разрабатывался на основе стандартов ГОСТ Р ИСО/МЭК 27002–2012 и ГОСТ Р ИСО/МЭК 15408-1-2012, ГОСТ Р ИСО/МЭК ТО 15446-2008 и ФСТЭК № 31 [3–6].

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: II квартал 2023 года // Positive Technologies. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/. – Загл. с экрана.

2. Бобылев, А. А. Определение уровня защищенности персональных данных и требований по их защите / А. А. Бобылев. – Электрон. текстовые дан. – Режим доступа: https://amgpgu.ru/upload/iblock/112/bobylev_a_a_opredelennie_urovnya_zashchishchennosti_personalnykh_dannykh_i_trebovaniya_po_ikh_zashch.pdf. – Загл. с экрана.

3. ГОСТ Р ИСО/МЭК 15408-1-2012. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Электрон. текстовые дан. – Режим доступа: https://docs.cntd.ru/document/1200101777. – Загл. с экрана.

4. ГОСТ Р ИСО/МЭК 27002-2012. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Электрон. текстовые дан. – Режим доступа: http://msiit.ru/x/miszki/____27002-2012.pdf. – Загл. с экрана.

5. ГОСТ Р ИСО/МЭК ТО 15446-2008. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. – Электрон. текстовые дан. – Режим доступа: https://docs.cntd.ru/document/1200075566. – Загл. с экрана.

6. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК от 14.03.2014 № 31. – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. – Загл. с экрана.

REFERENCES

1. Aktualnyye kiberugrozy: II kvartal 2023 goda [Current Cyber Threats: Second Quarter of 2023]. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/

2. Bobylev A.A. *Opredeleniye urovnya zashchishchonnosti personalnykh dannykh i trebovaniy po ikh zashchite* [Determination of Personal Data Security Level and Requirements for Their Protection]. URL: https://amgpgu.ru/upload/iblock/112/bobylev_a_a_opredelennie_urovnya_zashchishchennosti_personalnykh_dannykh_i_trebovaniya_po_ikh_zashch.pdf

3. *GOST R ISO/MEK 15408-1-2012. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy* [GOST R ISO/IEC 15408-1-2012. Security Methods and Responsibilities. Criteria for Assessing the Security of Information Technologies]. URL: https://docs.cntd.ru/document/1200101777

4. *GOST R ISO/MEK 27002-2012. Metody i sredstva obespecheniya bezopasnosti: Svod norm i pravil menedzhmenta informatsionnoy bezopasnosti* [GOST R ISO/IEC 27002-2012. Security Methods and Responsibilities: Code of Norms and Rules for Information Security Management]. URL: http://msiit.ru/x/miszki/____27002-2012.pdf

5. *GOST R ISO/MEK TO 15446-2008. Metody i sredstva obespecheniya bezopasnosti. Rukovodstvo po razrabotke profiley zashchity i zadaniy po bezopasnosti* [GOST R ISO/IEC TO 15446-2008. Safety Methods and Responsibilities. Guidelines for the Development of Protection Profiles and Safety Assignments]. URL: https://docs.cntd.ru/document/1200075566

6. *Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh obyektakh, potentsialno opasnykh obyektakh, a takzhe obyektakh, predstavlyayushchikh povyshennuyu opasnost dlya zhizni i zdorovya lyudey i dlya okruzhayushchey prirodnoy sredy: prikaz FSTEK ot 14.03.2014 № 31* [On Approval of Requirements for Information Protection in Automated Control Systems for Production and Technological Processes at Critically Important Facilities, Potentially Hazardous Facilities, and Facilities Endangering Human Life and Health and the Environment. FSTEC Order of March 14, 2014, No. 31]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

AUDIT OF SECURITY TOOLS FOR PERSONAL DATA INFORMATION SYSTEMS

Alexandra A. Danshina

Student, Department of Information Security,
Volgograd State University
danshina1955a@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security,
Volgograd State University
babenko.aleksey@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article proposes a model for conducting an external audit of the software and hardware parts of the organization. The statistics of the leakage of confidential information for the second quarter of 2023 are considered, as are the requirements for the information system for personal data, the levels of security of information, and the requirements for the protection of PDI. The article presents tasks implemented by the proposed model. The software package and its suggested requirements will minimize incidents in companies related to personal data leakage or unauthorized intrusions. The list of tasks for the audit program was developed on the basis of state standards. Information is a valuable resource, and its loss can affect the reputation and income of a business in various ways. That is why the problem of personal data protection has been and remains relevant. To reduce statistics on cyberattacks and identity theft, as well as to reduce the number of threats, vendors engaged in information security provide the market with more and more new solutions to ensure the protection of personal data every year. For example, security audits. Its purpose is to identify vulnerabilities, assess the effectiveness of existing information protection measures, and make recommendations to improve overall security.

Key words: audit of security tools, personal data, threat, security levels, software model.