

Е. О. Первякова^{1✉}, А. В. Троеглазова¹

Организация защиты конфиденциальной информации в химической лаборатории

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: ekaterinochka31@gmail.com

Аннотация. В данной статье анализируются актуальные вопросы обеспечения защиты информации химической испытательной лаборатории. Актуальность темы связана с необходимостью выполнения регламента законодательства Российской Федерации и международных стандартов при обработке конфиденциальной информации: ГОСТ ISO/IEC 17025-2019, Федеральный закон № 98-ФЗ, Федеральный закон № 152-ФЗ, Постановление Правительства № 1119, Приказ ФСТЭК России № 21. Опираясь на методику ФСТЭК установлены объекты воздействия, актуальные нарушители, потенциальные цели и сценарии осуществления угроз безопасности информации. Определены основные виды рисков и соответствующие им неблагоприятные исходы. Составлен список реальных угроз для общепринятой информационной системы персональных данных с четвертым уровнем защиты. Результаты данной работы можно применять при создании организационно-распорядительной документации и технических мер защиты в химических лабораториях.

Ключевые слова: коммерческая тайна, персональные данные, химическая лаборатория, модель угроз, уровень защищенности, информационная безопасность, ФСТЭК России, конфиденциальность

Е. О. Pervyakova^{1✉}, A. V. Troeglasova¹

Organization of confidential information protection in a chemical laboratory

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: ekaterinochka31@gmail.com

Abstract. This article analyzes the current issues of information protection in a chemical testing laboratory. The relevance of this topic is related to the need to comply with the regulations of the Russian Federation and international standards when processing confidential information: GOST ISO/IEC 17025-2019, Federal Law No. 98-FZ, Federal Law No. 152-FZ, Government Decree No. 1119, and Order of the Federal Service for Technical and Export Control No. 21. Based on the FSTEC methodology, the objects of influence, current violators, potential targets, and scenarios for implementing information security threats have been identified. The main types of risks and their corresponding adverse outcomes have been determined. A list of real threats has been compiled for a conventional information system with a fourth-level protection system. The results of this work can be used in the creation of organizational and administrative documentation and technical protection measures in chemical laboratories.

Keywords: trade secret, personal data, chemical laboratory, threat model, security level, information security, FSTEC of Russia, confidentiality

Введение

В современном мире основополагающая роль в гарантировании качества продукции и безопасности технологических процессов, связанных с химическими веществами и материалами, принадлежит испытательным лабораториям. Согласно ГОСТ ISO/IEC 17025-2019, значимым аспектом работы данных лабораторий выступает обеспечение конфиденциальности информации – коммерческой тайны и персональных данных [1].

В условиях рыночной экономики утечка сведений, составляющих коммерческую тайну, может привести к серьезным экономическим потерям и снижению конкурентоспособности. Таким же образом и разглашение персональных данных может привести не только к потере репутации, но и повлечь за собой административную, а иногда и уголовную ответственность. Несмотря на большое количество статей по защите информации, комплексные изучения, применяемые к специфике работы химических испытательных лабораторий, остаются представленными в неполной мере.

Цель работы – формирование подхода к выявлению актуальных рисков и подбору средств защиты коммерческой тайны и персональных данных в химической лаборатории. Задачи включают в себя: анализ нормативно-правовой базы, установление объектов воздействия, определение актуальных нарушителей и моделей угроз, аргументация степени защиты информационной системы персональных данных.

Методы и материалы

Методологическая основа данного исследования построена изучении методов системного анализа, классификации и моделирования угроз согласно методике ФСТЭК России от 5 февраля 2021 года «Методика оценки угроз безопасности информации» [2]. В статье были использованы положения, следующих нормативных правовых актов:

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [2].
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [3].
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [4].
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [5].

В качестве объекта исследования представлена общепринятая информационная система персональных данных (ИСПДн) химической испытательной лаборатории, и система обеспечения сохранности коммерческой тайны.

Результаты

Установлено, что защита коммерческой тайны в химической лаборатории должна содержать в себе четыре обязательных пункта:

1. определение списка информации, составляющей коммерческую тайну (результаты испытаний, данные о заказчиках, рабочие записи лаборатории и т.д.) и написание списка сотрудников, допускающихся к работе с конфиденциальной информацией;

2. создание внутренних локальных актов (Положение о коммерческой тайне, инструкции);

3. использование технических средств (шифрование, антивирусы, контроль доступа);

4. систематический внутренний аудит.

5. В разделе персональных данных для ИСПДн устанавливается 4-й уровень защищенности:

6. обрабатываются «иные» категории ПДн;

7. субъекты – только сотрудники лаборатории;

8. количество – любое;

9. актуальные угрозы принадлежат к 3-му типу (не зависят от недеklarированных возможностей ПО) (табл. 1).

Таблица 1. Уровень защищенности персональных данных

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 1	УЗ 2
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	сотрудники	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	сотрудники	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 3	УЗ 4
	сотрудники	Любое	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудники	Более 100 тыс.	УЗ 2	УЗ 2	УЗ 4
		Менее 100 тыс.	УЗ 2	УЗ 3	УЗ 4
	сотрудники	Любое	УЗ 2	УЗ 3	УЗ 4

Проанализировав объекты воздействия были идентифицированы: персонал (сотрудники), информационные активы (личные дела), АРМ сотрудников, носители информации (флешки, бумажные архивы), база данных, локальная сеть (рис. 1).

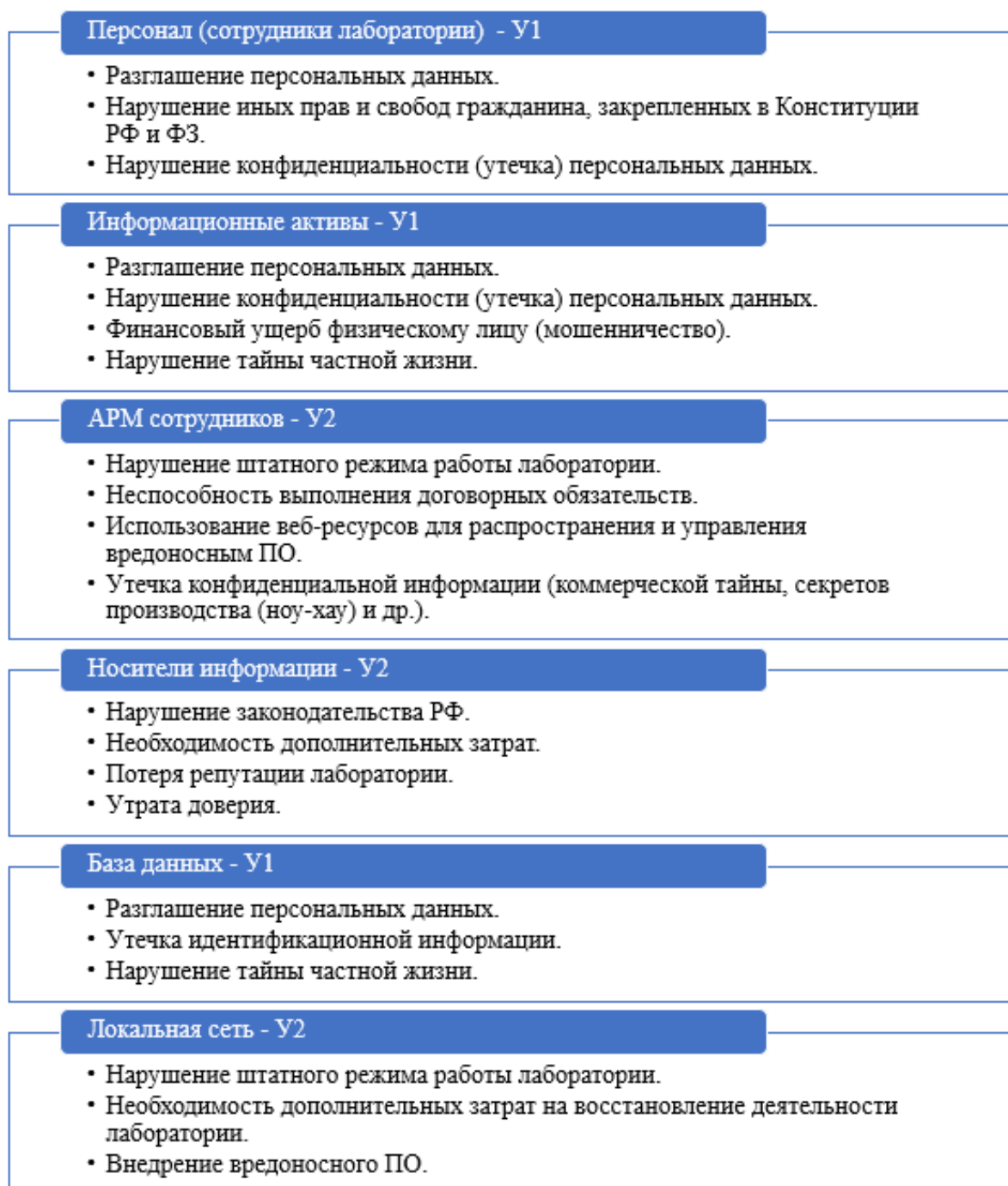


Рис. 1. Виды рисков и негативные последствия от реализации угроз безопасности информации

Также были выявлены категории нарушителей: от внешних (некоторые физические лица (хакеры), конкурирующие компании, бывшие сотрудники) до

внутренних (сетевые администраторы, авторизованные пользователи – кадровики, бухгалтера, лаборанты, а также разработчики ПО). Потенциал возможностей нарушителей варьируется от базового (Н1) до среднего (Н3).

С помощью матрицы соответствия были установлены актуальные угрозы безопасности информации (рис. 2.1.-2.3.) [6, 7].

УБИ.006 – Угроза внедрения кода или данных	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода.
УБИ.012 – Угроза деструктивного изменения конфигурации/среды окружения программ	Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками.
УБИ.023 – Угроза изменения компонентов информационной системы	Угроза заключается в возможности получения нарушителем доступа к сети, файлам, внедрения закладок путём несанкционированного изменения состава программных или аппаратных средств ИС.
УБИ.030 – Угроза использования информации аутентификации, заданной по умолчанию	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников или от информационного сервиса идентификационной и аутентификационной информации.
УБИ.033 – Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных.
УБИ.034 – Угроза использования слабостей протоколов сетевого/локального обмена данными	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе.
УБИ.086 – Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.

Рис. 2.1. Возможные угрозы

УБИ.088 – Угроза несанкционированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий.
УБИ.090 – Угроза несанкционированного создания учетной записи пользователя	Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях.
УБИ.091 – Угроза несанкционированного удаления защищаемой информации	Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации.
УБИ.098 – Угроза обнаружения открытых портов и идентификации сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам.
УБИ.099 – Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов.
УБИ.104 – Угроза определения топологии вычислительной сети	Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы для получения сведений о топологии дискредитируемой вычислительной сети.
УБИ.115 – Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств.
УБИ.116 – Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном или активном режиме для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз.
УБИ.122 – Угроза повышения привилегий	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс от его имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав.

Рис. 2.2. Возможные угрозы

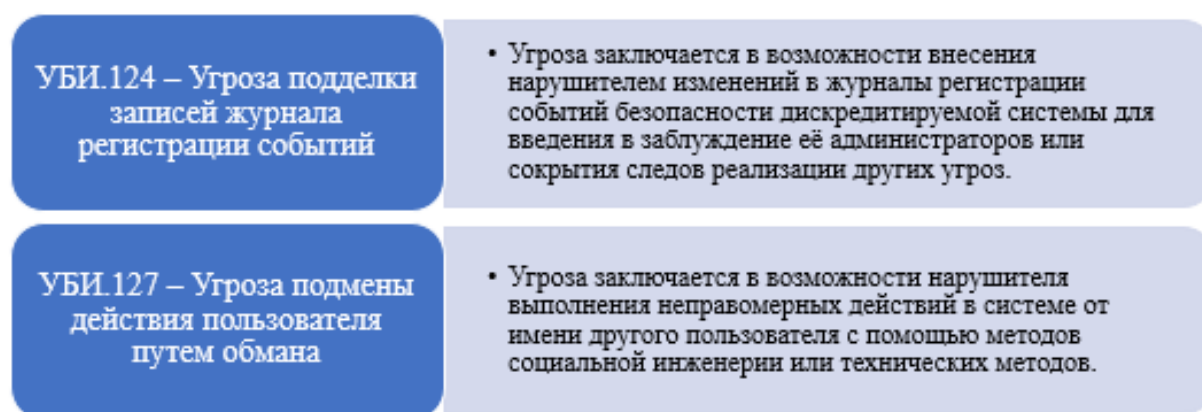


Рис. 2.3. Возможные угрозы

В результате установления 4-го уровня защищенности и модели угроз предложен комплекс мер, разделенный на три группы:

1) правовые меры:

- введение режима коммерческой тайны;
- назначение ответственного за обработку ПДн и получение согласий на обработку;

2) организационные меры:

- положение о коммерческой тайне;
- обязательство о неразглашении коммерческой тайны;
- инструкция по работе с конфиденциальной информацией;
- журнал учета носителей информации;
- акты уничтожения носителей;
- журнал учета ознакомления работников с Положением о коммерческой тайне;
- журнал учета выдачи и приема ключей от помещений/шкафов;
- инструкция о ходе действий при установлении утечки или разглашении коммерческой тайны;

3) технические меры:

- размещение и настройка межсетевого экрана на границе локальной сети;
- применение системы антивирусной защиты на всех АРМ;
- использование средств контроля съемных носителей;
- кодирование жестких дисков ноутбуков и АРМ;
- введение системы регистрации событий безопасности (журналы аудита доступа к файлам и БД);
- создание резервных копий базы данных (ежедневное копирование на внешний зашифрованный носитель и в облачное хранилище с соблюдением требований).

Заключение

В результате проделанной работы, был проведен системный анализ нормативно-правовой базы защиты коммерческой тайны и персональных данных относительно химической испытательной лаборатории. Опираясь на методику ФСТЭК, был выявлен четвертый уровень защищенности ИСПДн, определены объекты воздействия, актуальные нарушители и основные сценарии угроз, сформирован перечень из 18 актуальных угроз безопасности информации, детализированный по тактикам и техникам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Законы. О персональных данных: Федеральный закон № 152–ФЗ: [принят Государственной Думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года]. – Москва, 2021. – 36 с.
2. Российская Федерация. Законы. Методика оценки угроз безопасности информации: Методический документ: [утвержден Федеральной службой по техническому и экспортному контролю 5 февраля 2021 года]. – Москва, 2021. – 83 с.
3. Российская Федерация. Законы. О персональных данных: Федеральный закон № 152–ФЗ: [принят Государственной Думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года]. – Москва, 2021. – 36с.
4. Российская Федерация. Законы. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление правительства Российской Федерации № 1119: [утвержден Постановлением правительства Российской Федерации 1 ноября 2012 года]. – Москва, 2012. – 7с.
5. Российская Федерация. Законы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК № 21: [утвержден Приказом ФСТЭК России 18 февраля 2013 года]. – Москва, 2013. – 20 с.
6. ФСТЭК России: Банк данных угроз безопасности информации: официальный сайт. – Москва. – URL: <https://bdu.fstec.ru/threat> (дата обращения: 24.03.2026). – Текст: электронный.
7. Российская Федерация. Законы. Методика оценки угроз безопасности информации: Методический документ: [утвержден Федеральной службой по техническому и экспортному контролю 5 февраля 2021 года]. – Москва, 2021. – 83 с.

© *Е. О. Первякова, А. В. Троеглазова, 2026*