УДК 528.71
DOI 10.33764/2618-981X-2023-6-153-159

А. А. Литвяков[1]*, *И. Н. Карманов*[1]

Оценка риска нарушения конфиденциальности информации с использованием лазерных систем разведки

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: mr.go_old@mail.ru

Аннотация. Статья посвящена исследованию потенциальных угроз и уязвимостей нарушения конфиденциальности информации с использованием лазерных систем разведки на основе банка данных угроз Федеральной Службы технического и экспортного контроля. В статье проводится анализ возможных угроз и уязвимостей, связанных с применением лазерных систем разведки, включая возможность несанкционированного доступа к конфиденциальным данным, перехвата информации, нарушения конфиденциальности передачи данных и других аспектов информационной безопасности. Базируясь на банке данных угроз Федеральной Службы технического и экспортного контроля, выделяются определенные категории угроз и уязвимостей. В заключении статьи предлагаются рекомендации по предотвращению и минимизации рисков нарушения конфиденциальности информации с использованием лазерных систем разведки.

Ключевые слова: лазерные системы разведки, угрозы, уязвимости, конфиденциальная информация, информационная безопасность

A. A. Litvyakov[1]*, *I. N. Karmanov*[1]

Assessment of the Risk of Violating the Confidentiality of Information Using Laser Reconnaissance Systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: mr.go_old@mail.ru

Abstract. The article is devoted to the study of potential threats and vulnerabilities of breaking confidential information using laser reconnaissance systems based on the threat data bank of the Federal Service for technical and export control. The article analyzes possible threats and vulnerabilities associated with the use of laser reconnaissance systems, including the possibility of unauthorized access to confidential data, interception of information, violation of the confidentiality of data transmission and other aspects of information security. Based on the threat data bank of the Federal Service for technical and export control, certain categories of threats and vulnerabilities are distinguished. In conclusion, the article offers recommendations for preventing and minimizing the risks of breaching confidential information using laser reconnaissance systems.

Keywords: laser reconnaissance systems, threats, vulnerabilities, confidential information, information security

Введение

С развитием технологий лазерные системы разведки становятся все более распространенным средством хищения конфиденциальной информации. Такие системы представляют шанс реализации потенциальных угроз и уязвимостей,

связанных с нарушением конфиденциальности передачи данных, несанкционированным доступом и перехватом информации.

Цель данной статьи – провести исследование потенциальных угроз и уязвимостей нарушения конфиденциальной информации с использованием лазерных систем разведки на основе банка данных угроз Федеральной Службы технического и экспортного контроля (БДУ ФСТЭК). БДУ ФСТЭК является руководством, разработанным ФСТЭК России, и содержит рекомендации и требования по обеспечению информационной безопасности в различных сферах деятельности.

В данной статье проводится анализ возможных угроз и уязвимостей, связанных с применением лазерных систем разведки, на основе БДУ ФСТЭК. Были выделены основные категории угроз и уязвимостей и проведена оценка. Затем, на основе анализа, предложены рекомендации по предотвращению и минимизации рисков нарушения конфиденциальной информации при использовании лазерных систем разведки.

Методы и материалы

Осуществить перехват речевой информации внутри помещений возможно с помощью лазерных средств акустической разведки, используя дистанционное лазерно-локационное зондирование объектов, обладающих свойствами, которые позволяют их использовать в качестве потенциальных источников закрытой речевой информации. Такими объектами могут быть, например, оконные стекла и другие виброотражающие поверхности [2].

Данный метод основывается на использовании лазерных лучей для измерения вибраций, возникающих на поверхности этих объектов в ответ на звуковые волны, создаваемые голосом людей внутри помещения. Измеренные вибрации преобразуются обратно в звуковые волны, что позволяет перехватывать и записывать речевую информацию [1].

На рис. 1 представлена схема утечки речевой информации с использованием лазерных систем разведки.

На сегодняшний день существует множество различных систем лазерной акустической разведки, которые позволяют перехватывать звуковую информацию на расстоянии от нескольких десятков метров до нескольких километров. Например, система SIPE LASER 3-DA SUPER [3] включает в себя гелий-неоновый лазер, блок фильтрации шумов, головные телефоны, аккумулятор и штатив для установки оборудования.

Для наведения лазерного излучения на нужное окно используется телескопический визир, а специальная оптическая насадка позволяет регулировать угол расходимости светового пучка [7]. Система обеспечивает высокое качество перехвата речевой информации на расстоянии до 250 метров [3].

Из современных систем лазерной акустической разведки особое внимание стоит обратить на следующие модели [3]:

– «Икар» (Icar) – это система, разработанная компанией «Лазерный инженеринг» (Laser Engineering) [3], которая может обнаруживать и идентифициро-

вать звуки, создаваемые различными видами вычислительной техники, на расстоянии до 2 км. Она использует технологию измерения времени задержки отраженных звуковых волн, чтобы определить расстояние до источника звука;

– «акула» (Akula) – это система, разработанная компанией «Российская электронная техника» (Russian Electronic Technology), которая использует лазерное излучение для обнаружения и анализа звуковых волн на расстоянии до 2 км. Она может использоваться для обнаружения и идентификации транспортных средств, определения местоположения стрелков и детектирования звуковых сигналов в акустических областях;

– «комплекс-24» (Complex-24) – это система, разработанная компанией «Технологии лазерной микрообработки» (Laser Microprocessing Technologies), которая может обнаруживать звуковые сигналы на расстоянии до 5 км. Она использует лазерное излучение для измерения времени задержки отраженных звуковых волн, чтобы определить расстояние до источника звука.

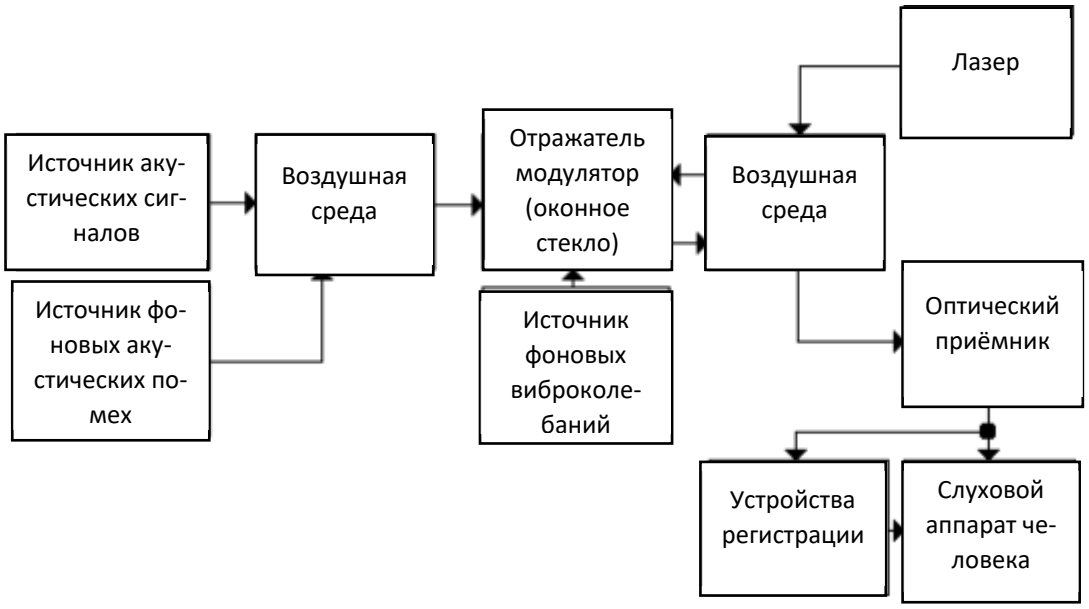

Рис. 1. Обобщенная схема утечки информации по оптико-акустическому каналу

Другим примером является лазерное устройство НРО150 [3], которое также использует гелий-неоновый лазер в качестве передатчика, а также блок компенсации помех и кассетное устройство магнитной записи в составе приемника. Это устройство обладает дальностью ведения разведки до 1000 метров [3].

Однако, устройства лазерной акустической разведки сталкиваются с высокими требованиями к помехоустойчивости, так как качество перехватываемой информации напрямую зависит от уровня фоновых шумов, помеховых вибраций отражателя-модулятора, а также ослабления лазерного излучения в атмосфере и фоновой оптической засветки при приеме отраженного от объекта сигнала [4].

Для оценки риска нарушения конфиденциальности информации с использованием лазерных систем разведки, на основе БДУ ФСТЭК, были выделены угрозы, представленные в табл. 1. [5].

Согласно ГОСТ Р 58771-2019 «Спецификация системы управления информационной безопасностью», уровень риска вычисляется с учетом следующих показателей: ценности ресурса, уровня угрозы и степени уязвимости. С увеличением значений этих параметров риск возрастает. Таким образом, формулу можно представить в следующем виде [10]:

$$R = AV \times EF \times ARO, \quad (1)$$

где AV (Asset Value, AV) – ценность актива (ресурса). Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 – минимальная стоимость ресурса, 2 – средняя стоимость ресурса и 3 – максимальная стоимость ресурса [10]; *EF* (Exposure Factor, *EF*) – уровень угрозы (мера уязвимости ресурса к угрозе). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 – минимальная мера уязвимости (слабое воздействие), 2 – средняя (ресурс подлежит восстановлению), 3 – максимальная (ресурс требует полной замены после реализации угрозы) [10]; *ARO* (Annual Rate of Occurrence, *ARO*) – уровень (оценка вероятности реализации угрозы) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая) [10].

Таблица 1

Угрозы безопасности информации

Угроза	Наименование угрозы	Потенциал нарушителя	Последствия реализации угрозы	Качественный показатель риска (*ARO*)
УБИ. 132	Угроза получения предварительной информации об объекте защиты	Средний	Нарушение конфиденциальности	3
УБИ. 139	Угроза преодоления физической защиты	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	3
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	3

Угроза	Наименование угрозы	Потенциал нарушителя	Последствия реализации угрозы	Качественный показатель риска (*ARO*)
УБИ. 203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Средний	Нарушение конфиденциальности	3
УБИ. 080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	2
УБИ. 085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Средний	Нарушение конфиденциальности	2
УБИ.111	Угроза передачи данных по скрытым каналам	Средний	Нарушение конфиденциальности	3

Таким образом, можно рассчитать качественный показатель риска представленных угроз: в случае использования лазерной системы разведки, вероятность реализации каждой из угроз возрастает до максимального значения – показатель *ARO* = 3. Исключением являются УБИ 80 и УБИ 85, так как хоть и при использовании лазерной системы разведки существует вероятность считывания сигналов компьютера или звуков нажатия клавиш, однако такие данные довольно сложно расшифровать и использовать.

Результаты

В табл. 2 представлены результаты вычислений качественного показателя риска. С учетом максимальных значений расчета, наивысший показатель равен 27 пунктам. График качественного значения показателя риска приведен на рис. 2.

Из рис. 2 видно, что большинство угроз имеет средний уровень риска и выше. Это говорит о том, что применение мер по снижению рисков хищения конфиденциальной информации с использованием лазерных систем разведки является оправданным и необходимым.

Таблица 2

Расчет качественного значения риска

Угроза	Показатель *AV*	Показатель *EF*	Значение риска *R*
УБИ. 132	1	2	6
УБИ. 139	2	2	12
УБИ. 187	2	3	27
УБИ. 203	2	3	18
УБИ. 080	3	3	18
УБИ. 085	3	3	18
УБИ.111	3	3	27

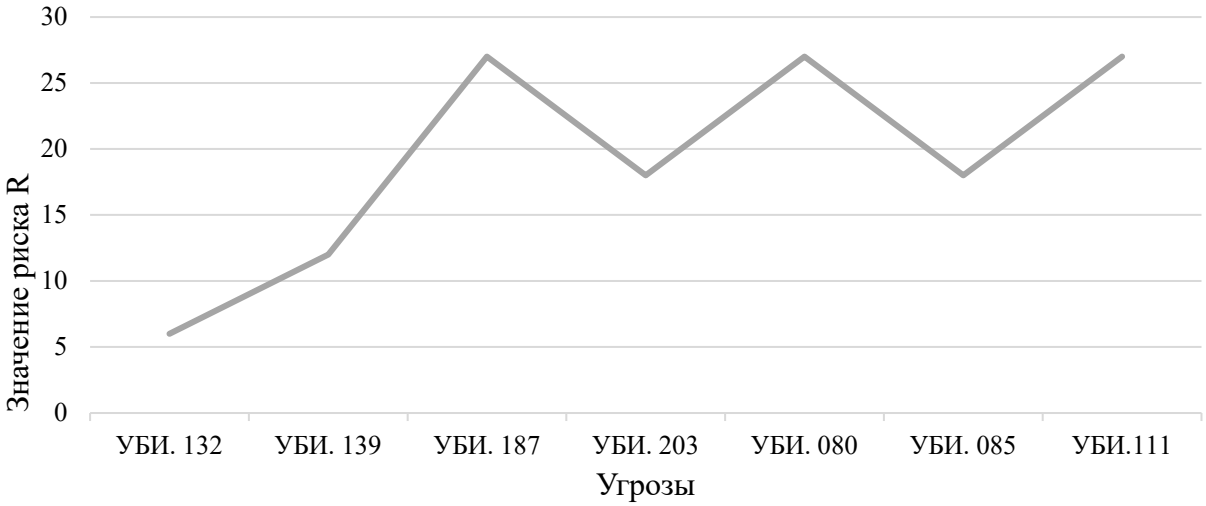

Рис. 2. График качественного значения показателя риска

Заключение

В ходе исследования была проведена качественная оценка рисков утечки конфиденциально информации по акустооптическому каналу. По результатам оценки стало ясно, что применение мер по снижению представленных рисков является оправданным, необходимым и окупаемым.

Для того, чтобы снизить риск утечки информации по акустооптическому каналу рекомендуется:

– ограничить доступ к зонам, где может быть применена лазерная система разведки;

– использовать специальные средства защиты, такие как экранирующие устройства или оптические фильтры;

– проводить регулярные проверки на наличие утечек конфиденциальной информации с помощью специального оборудования;

– обучать персонал правильной процедуре обращения с конфиденциальной информацией и предоставлять инструкции по использованию специальных устройств защиты;

– организовывать регулярное техническое обслуживание и проверку на наличие возможных уязвимостей и угроз в системах безопасности [6].

Благодарности

Авторы выражают благодарность Федеральной службе по техническому и экспортному контролю за предоставленные данные и информацию, необходимые для проведения исследования и написания данной статьи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ярочкин В.И. Технические каналы утечки информации. – М.: ИПКИР, 1994. – 102 с.

2. Лаврухин Ю.Н. Проблемы технической защиты конфиденциальной информации / Ю.Н. Лаврухин // Информация и безопасность: материалы межрегиональной научно-практической конференции. – Вып.2. – Воронеж: ВГТУ, 2002. – С. 14–16.

3. Андрианов В.И., Бородин В.А., Соколов А.В. Шпионские штучки и устройства для защиты объектов и информации. Справочное пособие. – СПб.: Лань, 1998. – 272 с.

4. Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. М.: РЦИБ Факел, 2008. 256 с.

5. Официальный сайт банка данных угроз ФСТЭК России. – [Электронный ресурс] –Режим доступа: https://bdu.fstec.ru/threat (дата обращения 24.04.2023).

6. Управление рисками по ITIL [Электронный ресурс]. – Режим доступа: https://www.itexpert.ru/rus/ITEMS/77-33/ (дата обращения 22.04.2023).

7. Зайцев А.П. Технические средства и методы защиты информации: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. - М.: ГЛТ , 2012. - 616 с.

8. Учаев Д.Ю., Брумштейн Ю.М., Ажмухадедов И.М., Князева О.М., Дюдиков И.А. Анализ и управление рисками, связанными с информационным обеспечением человеко-машинных АСУ технологическими процессами в реальном времени // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 82–97.

9. Методический документ. "Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021) – [Электронный ресурс] – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения 26.04.2023)

10. Национальный стандарт Российской Федерации «Менеджмент риска. Технологии оценки риска» ГОСТ Р 58771-2019 (введен 01.03.2020) [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200170253 (дата обращения 27.09.2021).