УДК 004.054
DOI 10.33764/2618-981X-2024-6-115-120

О. О. Крупко[1], А. В. Шабурова[1]*

Аудит информационной безопасности и его методы в управлении информационной безопасностью организации

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: olesyakrupko4@gmail.com

Аннотация. Автоматизированные системы имеют важное значение для эффективного функционирования коммерческих и государственных организаций. В данной статье рассматривается проблема управления информационной безопасностью организации. Для решения этой проблемы предлагается выполнение систематического аудита. Целью статьи является определение термина, его суть и технология проведения аудита информационной безопасности. В статье рассказывается о трудностях, с которыми можно столкнуться при подготовке к аудиту. Принимая во внимание то, что в современном мире всё больше увеличивается количество атак на информационные системы организаций, важно постоянно контролировать актуальность систем безопасности в соответствии с текущими угрозами, своевременно выявлять новые уязвимости и обеспечивать надежную защиту этих систем. В статье определены методы и ступени проведения аудита информационной безопасности, а также ориентиры оценивания результатов аудита.

Ключевые слова: информационная безопасность, аудит информационной безопасности, этапы проведения аудита

O. O. Krupko[1], A. V. Shaburova[1]*

Information security audit and its methods in managing the information security of an organization

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: olesyakrupko4@gmail.com

Abstract. Automated systems are essential for the effective functioning of commercial and government organizations. This article discusses the problem of managing the information security of an organization. The solution to this problem is to perform a systematic audit. The purpose of the article is to define the term, its essence and technology of information security audit. The article talks about the difficulties that you may encounter when preparing for an audit. Taking into account the fact that in the modern world the number of attacks on the information systems of organizations is increasing, it is important to constantly monitor the relevance of these security systems in accordance with current threats, promptly identify new vulnerabilities and ensure reliable protection of systems. The article defines the methods and stages of conducting an information security audit, as well as guidelines for evaluating audit results.

Keywords: information security, information security audit, audit stages

Введение

Важным аспектом в обеспечении защиты информационных ресурсов предприятия является аудит информационной безопасности. Объективная оценка уровня защищённости информационных систем необходима для эффективной защиты предприятия, собственно для этого и используется аудит [1]. Вот несколько причин, почему он является важным элементом:

– обнаружение потенциальных уязвимостей, что позволяет своевременно принять меры по их устранению;

– проверка системы защиты на соответствие законодательству;

– мониторинг действий сотрудников и контроль разграничения доступа сотрудников к информации.

Исходя из этого, можно сделать вывод, что для защиты предприятия от потери данных, нарушения конфиденциальности и других атак, связанных с нарушением безопасности, необходим аудит информационной безопасности.

Понятие и сущность аудита

Аудит безопасности представляет собой проверку и оценку документов, мероприятий и другой деятельности организации, которая потенциально может рассматриваться как относящуюся к умышленным атакам. Такие проверки призваны повысить уровень безопасности информации и воздержаться от излишних технических средств обеспечения информационной безопасности.

В ГОСТе Р 53114-2008 приведено определение аудита информационной безопасности организации [2]. Аудит не может проводиться без конкретной задачи, он всегда направлен на определённую цель [3].

В настоящее время определены следующие основные методы проведения аудита информационной безопасности [4]:

– аудит на соответствие нормативным документам;

– активный аудит, позволяет оценить степень защищённости по мнению злоумышленника;

– экспертный аудит, позволяет оценить степень защищённости в сравнении с «идеальной» системой защиты [5].

Источники угроз, которые приводят к нарушению целостности, доступности или конфиденциальности информации, можно разделить на несколько групп [6]. К первой группе относятся целенаправленные действия злоумышленников, а иногда и сотрудников этой организации, желающих получить выгоду. Ко второй группе относятся неосторожные, легкомысленные действия сотрудников, которые открывают непроверенные файлы или посещают заражённые сайты. К третьей группе источников угроз относится использование недостаточных средств технической защиты информации: отсутствие антивирусов, средств контроля и управления доступом или охранной сигнализации. Ещё одной немаловажной составляющей является отслеживание изменений законодательства и требований руководящих документов ФСТЭК. Также к отдельной группе можно отнести несчастные случаи и стихийные бедствия.

Комплекс мероприятий по обнаружению этих источников угроз для определённого предприятия и есть аудит. Предприятия оптико-электронной промышленности относятся к субъектам критической информационной инфраструктуры, и в соответствии с законом для них является обязательным проведение категорирования. Категорирование позволяет произвести правильную расстановку приоритетов при организации системы информационной безопасности [7].

Методы и ступени проведения аудита информационной безопасности

Выбор метода аудита зависит от целей и степени риска для организации. Для небольших компаний, интерес злоумышленников к которым снижен, характерно использование менее продвинутых технологий защиты информации, соответственно и оценка упрощается. Основополагающим условием для начала аудита является написание технического задания для имеющейся системы информационной безопасности. Аудитору необходимо понимать, как должна работать идеальная система безопасности в понимании руководителя.

Аудит можно разделить на ступени его выполнения [8]. Первой ступенью является очерчивание границ и степень глубины обследования организации, определяются области для проведения более тщательной оценки и области, которые обследуются не так глубоко. Это необходимый этап, т.к. аудит всех направлений организации является финансово затратным, а экономическая эффективность применения полученных в ходе аудита данных может оказаться невелика.

На второй ступени проведения аудита изучаются информационные процессы и создаётся перечень всех программных и технических средств

Третья ступень обширная и включает в себя много вопросов, упускать которые нежелательно [9]. Этот этап анализа процессов происходит на рабочих местах сотрудников и состоит из:

– анализа работы персонала с данными;

– анализа порядка вводного инструктажа по правилам безопасности для новых сотрудников и регулярных повторных инструктажей для всего персонала;

– анализ систем контроля и управления доступом, а также сотрудников, управляющих доступом;

– анализ фактического наличия документов, регламентирующих отнесение документов к информации ограниченного доступа, и порядок работы с такими документами;

– анализ систем обеспечения защиты от вредоносных программ;

– анализ отслеживания и реагирования на инциденты в сфере информационной безопасности;

– анализ использования алгоритмов шифрования;

– анализ процессов сбора, хранения, обработки и уничтожения информации;

– анализ того, как используются съёмные устройства хранения данных;

– анализ организации подключения и использования ресурсов интернета, а также организации удалённого доступа сотрудников.

На четвёртой ступени происходит оценка технического и программного обеспечения, в том числе проверка физических средств защиты, таких как сейфы, экраны, жалюзи, замки и другие.

Пятая ступень заключается в сравнение имеющейся системы с «идеальной» системой для данного предприятия, в ходе выполнения этапа выявляются уязвимости и определяются риски.

Шестая, последняя, ступень заключается в составлении отчёта для руководителя, в котором указано, какие недостатки системы безопасности были выявлены, и их опасность.

Как оценивать результаты аудита информационной безопасности

Основным ориентиром оценивания результатов аудита является международный стандарт ISO/IEC 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», либо его национальный аналог ГОСТ Р ИСО/МЭК 27001-2021 [10], стандарт ISO/IEC 27002 «Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью», содержит рекомендации для организаций для улучшения системы управления информационной безопасностью. Также по результатам аудита можно оценить соответствие требованиям руководящих документов ФСТЭК по управлению информационной безопасностью или соответствие компании определённым стандартам, например, международный стандарт безопасности PCI DSS, стандарт безопасности AICPA SOC или набор рекомендаций по созданию надежной системы безопасности для ПО на базе Kubernetes.

Отчет по результатам аудита составляется аудитором на основании своего опыта, оценивая применимость этих требований к обследуемой организации.

Из отчета по результатам аудита руководитель также может определить порядок устранения угроз, в соответствии с их значимостью. Кроме того, исполнитель аудита может указать в отчете как скоро необходимо устранить угрозы [11].

В случае выбора любого подхода проведения аудита ключевые этапы остаются неизменными (рис. 1).

Рис. 1. Основные этапы работ при проведении аудита безопасности

Результаты

Результаты проведения аудита всегда формируются в отчёт, в котором описываются обнаружившиеся проблемы и рекомендуемые способы для их устранения.

Так, в отчете должны быть отражены следующие итоги:

– объективная оценка действительного состояния информационной безопасности в организации;

– уязвимости, выявленные в ходе аудита и оценка их опасности;

– перечень мер, рекомендованных для повышения уровня защищённости;

– вывод о соответствии (несоответствии) стандартам организации и требованиям отрасли;

– подтверждение эффективности существующей системы защиты.

Заключение

Аудит информационной безопасности позволяет выявить уязвимости, оценить соответствие стандартам текущей системы информационной безопасности, повысить эффективность используемых мер защиты информации. Регулярно проводимый аудит даёт реальную пользу. Информация, полученная при регулярном проведении аудита, помогает разрабатывать и совершенствовать стратегию информационной безопасности предприятия, чтобы она соответствовала современным угрозам и требованиям. Таким образом аудит представляет собой важный процесс для обеспечения эффективной и надёжной системы информационной безопасности организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Багров Е. В. Мониторинг и аудит информационной безопасности на предприятии // NBI-technologies. 2011. – №5. – С. 54-56.

2. ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации. Основные термины и определения. – М., 2008. – 20 с. (Защита информации).

3. Хлестова Д. Р., Байрушин Д. Р. Аудит информационной безопасности в организации // Символ науки. 2016. – №11-3. – С. 175-177.

4. Вакуленко А. А., Сорокопудов Н. С., Коваленко Б. Б. Инструменты выбора метода аудита информационной безопасности предприятия // Экономика и экологический менеджмент. – 2019. – №3. – С. 163-168.

5. Просянников Р. Е. Избавиться от заблуждений. Виды аудита информационной безопасности // Connect! Мир связи. – 2004. – № 12. – С. 148-151.

6. Хватов Д. А., Ковтун А. И., Подтопельный В. В. Проблемы аудита информационной безопасности АСУ ТП // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. – 2019. – №4. – С. 67-75.

7. Оюн Ч. О., Попантонопуло Е. В. Объекты критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. – 2018. – № 9. – С. 45-49.

8. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. – 2018. – №1. – С. 1-29.

9. Двойнишников Н. Э., Исламутдинова Д. Ф. Понятие и сущность аудита безопасности информационных систем // Московский экономический журнал. – 2019. – №10. – С. 98-101.

10. ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности Требования. – М., 2006. – 26 с. (Информационная технология).

11. Аверченков В. И. Аудит информационной безопасности : учеб. пособие 3-е изд., стер. М. : ФЛИНТА, – 2016. – 269 с.