Секция «Компьютерное право и информационная безопасность»

Аудит информационной безопасности

Научный руководитель – Дубровина Оксана Васильевна

Боки́й Елизавета Сергеевна
Студент (специалист)
Тамбовский государственный технический университет, Тамбовская область, Россия
E-mail: elizaveta6903@mail.ru

В настоящее время вопросам информационной безопасности организации уделяется особое внимание. Атаки хакеров, сбои в работе программ, распространение вирусов и многие другие уязвимости систем информационной безопасности делают проблему защиты информации первостепенной. Но важно не просто защитить информацию, систему информационной безопасности необходимо постоянно проверять и поддерживать в рабочем состоянии. Для этих целей проводится аудит информационной безопасности организации.

Под аудитом информационной безопасности понимается полная проверка всех параметров и составляющих информационной безопасности в организации, включая информационные системы, программно-аппаратный и инженерно-технический комплексы защиты информации [2].

Аудит должен быть всесторонним и полным, что позволит вовремя обнаружить проблемы в системе информационной безопасности и избежать рисков и потерь информации, что в свою очередь ведет не только к потере данных, но и финансовым потерям.

Аудит информационной безопасности включает в себя проведения внутреннего и внешнего аудита. Внутренний аудит проводится силами сотрудников отдела безопасности и состоит в плановой проверке всех параметров работы системы и составлении отчета по ее результатам. Внешний аудит проводят специалисты сторонних организаций, предоставляющих услуги по аудиту информационной безопасности.

Для проведения полного аудита необходимо оценить все имеющиеся активы конфиденциальной информации, все обрабатывающие эту информацию системы и провести полный учет системы информационной безопасности организации на соответствие ее действующим нормативно-правовым и законодательным актам [1].

На основании оценки определяется текущий уровень защищенности информации, происходит расчет всех возможных угроз информационной безопасности и составляется перечень актуальных угроз.

Результатом проведения аудита информационной безопасности является список рекомендаций и предложений по совершенствованию мер защиты. На основании этих предложений отделом информационной безопасности устраняются все возможные уязвимости системы. После этого происходит тестирование системы.

Таким образом аудит информационной безопасности является важной составляющей защиты информации. Для поддержания всей системы информационной безопасности в работоспособном состоянии аудит необходимо проводить не менее двух раз в год.

Нормативно-правовая база проведения аудита информационной безопасности опирается на имеющиеся стандарты и документы, регламентирующие обеспечение информационной безопасности в целом. Методики проведения аудита разработаны для банковских и финансовых систем, но на их основе в настоящее время проводится аудит всех организаций. В качестве развития этого вопроса назревает необходимость в четкой регламентации процедуры аудита информационной безопасности для всех сфер деятельности.

Источники и литература

1) Информационно-правовой портал Гарант – [Электронный ресурс] – Режим доступа: https://garant.ru.
2) Сайт ФСТЭК России – [Электронный ресурс] – Режим доступа: https://fstec.ru.