УДК 004.056

Гильманова Э.А.
Магистрант ФГБОУ ВО «КГЭУ»
г. Казань, Россия

Ахметшина Р.И.
Магистрант ФГБОУ ВО «КГЭУ»
г. Казань, Россия

Научный руководитель:
Исмагилов И.Р.
кандидат технических наук, доцент, ФГБОУ ВО «КГЭУ»
г. Казань, Россия.

РОЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация

В статье рассматривается роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры. Обозначены преимущества использования проведения аудита информационной безопасности для субъекта КИИ.

Ключевые слова

Информационная безопасность, аудит, критическая информационная инфраструктура, система обеспечения информационной безопасности

Gilmanova E.A.
Master's student of FGBOU VO «KGEU»
Kazan, Russia
Akhmetshina R.I.
Master's student of FGBOU VO «KGEU»
Kazan, Russia
Scientific supervisor:
Ismagilov I.R.
Candidate of Technical Sciences, Associate Professor
of FGBOU VO «KGEU», Kazan, Russia.

THE ROLE OF INFORMATION SECURITY AUDIT IN THE LIFE CYCLE OF THE INFORMATION SECURITY SYSTEM OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Annotation

The article discusses the role of information security audit in the life cycle of the information security system for critical information infrastructure facilities. The advantages of using the information security audit for the subject of the CII are indicated.

Keywords

Information security, audit, critical information infrastructure, information security system

Информационные системы (ИС) в нынешних реалиях являются для государственных и коммерческих компаний основной частью обеспечения их продуктивной деятельности. Они во многих местах применяются для хранения, обработки и передачи данных, в связи с чем проблемы безопасности ИС весьма актуальны на сегодняшний день.

Нарушение работы субъектов КИИ способствует возникновению серьезных последствий и для конкретных организаций, и для государства в общем. Поэтому Правительство старается предпринимать меры, которые направлены на

обеспечение безопасности КИИ, а именно создает новые законодательные акты, методики с требованиями к безопасности. На сегодняшний день кибербезопасность находится под угрозой высоко осведомленных в области IT преступников, деятельность которых вполне может добраться до государственного уровня. Таким образом, актуальность обеспечения безопасности КИИ должна обязательно учитываться государственными структурами и бизнесом. Это необходимо, поскольку с каждым годом все больше становится данных, утечка которых способна сильно навредить безопасности страны [1, с.1446-1447].

Для безопасности субъектов КИИ от подобных атак нужно оценить степень защиты ее информационной системы. Такая работа проводится с помощью соответствующей проверки, а именно аудиторской [3, с.15].

Аудит ИБ (информационной безопасности) – способ контроля уровня защиты информационных активов организации. Услуга может предоставляться и для общего IT-аудита, и как самостоятельный проект. Очень часто аудит проводится как одно из мероприятий по созданию системы обеспечения информационной безопасности (СОИБ), при этом играет роль начального этапа реализации проекта.

При осуществлении аудита информационной безопасности применяются два вида исследований: организационно-методическое и техническое.

Чаще всего для него используются услуги сторонних организаций, которые работают в области информационной безопасности. Инициировать аудит может руководитель организации, служба ИБ или автоматизации. В рамках этой процедуры уровень безопасности оценивает экспертная группа, которая определяется с учетом обозначенных задач и особенностей объекта КИИ [5, с.3 - 5].

За счет аудита информационной безопасности можно получить адекватную оценку ситуации с обеспечением ИБ, и при выполнении полученных рекомендаций клиент может сделать защиту информационных ресурсов более эффективной и обезопасить инфраструктуру.

Заказчик процедуры аудита получает следующие плюсы:

1) Независимые эксперты оценивают степень защиты инфраструктуры IT. По итогам подобного исследования специалисты высокого уровня готовят для заказчика организационные мероприятия по возрастанию надежности и эффективности процессов, обеспечивающих информационную безопасность [2, с.5-8];

2) Используя полученные рекомендации, организация-заказчик оптимизирует свою IT-инфраструктуру и бизнес-процессы с учетом актуальных отраслевых требований, предъявляемых к ИБ;

3) Данная процедура позволяет надежнее защитить информацию, в том числе от утечки, снизить негативное влияние человеческого фактора и обеспечить ее доступность, целостность и конфиденциальность. Безопасность растет на всех уровнях: отдельного приложения, операционной системы, физической, виртуальной, сетевой инфраструктур и т.д;

4) Аудит дает возможность уменьшить расходы на обеспечение информационной безопасности и IT в общем, потому что по итогам услуги клиент получает рациональные советы, подготовленные с учетом особенностей инфраструктуры его компании;

5) Снижается риск утраты репутации вследствие недостаточного обеспечения информационной безопасности [4, с.7].

Благодаря аудиту выявляются уязвимые места, недостатки. Его процесс занимает важное место в росте качества создаваемых ИТ-решений, а также в снижении количества инцидентов, связанных с негативным воздействием на объект КИИ.

Исходные данные, полученные в ходе аудита, используются для анализа рисков ИБ, моделирования угроз, проектирования архитектуры СОИБ, основанной на рекомендациях по мерам обеспечения ИБ, сформированных на этапе аудита. Качество проведенного аудита оказывает влияние на принятие правильных решений по выбору и обоснованию средств защиты информации.

Список использованной литературы

1. Горелик В.Ю, Безус М.Ю. О безопасности критической информационной инфраструктуры Российской федерации // Научно-образовательный журнал «StudNet» №9/2020. С. 1446-1447

2. Автоматизация аудита. Н.В.Гомолко // [Электронный ресурс]. Режим доступаhttp://www.bseu.by:8080/bitstream/edoc/84963/1/Gomolko_N.V._367_370.pdf (дата обращения: 14.01.2022).

3. Кузнецов П.У. Отдельные аспекты формирования правового обеспечения международной информационной безопасности // Вестн. УрФО. 2016. № 4 (22). С. 38–43.

4. За 12 лет утекло более 30 млрд записей персональных данных // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/analytics/digest/15281/ (дата обращения: 27.11.2021).

5. Сердюк В.Д. Аудит информационной безопасности (ИБ) [Электронный ресурс]. URL: http://www.bytemag.ru/articles/detail.php?ID=6781 (Дата обращения 15.01.2022 г.)