Читалов М.В., Базанов Д.Б. Основы проведения комплексного риск-ориентированного аудита информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 7(33) с. 9–15

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ОСНОВЫ ПРОВЕДЕНИЯ КОМПЛЕКСНОГО РИСК-ОРИЕНТИРОВАННОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Читалов М.В., Базанов Д.Б.
ФГБОУ ВО "Российский экономический университет имени Г.В.Плеханова», Москва, Россия (115054, Москва, Стремянный переулок, д.36.), e-mail: [1]chitalov@vk.com

В современном мире непрерывно увеличивается число информационных активов. Вместе с этим предпринимаются попытки цифровой трансформации практически на каждом современном предприятии. Совокупность данных факторов актуализирует проблему, связанную с обеспечением информационной безопасности предприятия. Цель текущей статьи заключается в рассмотрении ключевых вопросов относительно проведения риск-ориентированного аудита информационной безопасности в контексте комплексного обеспечения защиты информации. Научная значимость работы состоит в возможности использования представленных материалов для формирования

Ключевые слова: Информация, информационная безопасность, аудит, риск-ориентированный подход, защита информации.

FUNDAMENTALS OF CONDUCTING A COMPREHENSIVE RISK-BASED AUDIT OF INFORMATION SECURITY

[1]Chitalov M.V., Bazanov D.B.
"Plekhanov Russian University of Economics", Moscow, Russia (117997, Moscow, Stremyanny Lane, 36), e-mail: [1]chitalov@vk.com

In the modern world, the number of information assets is continuously increasing. At the same time, attempts are being make at digital transformation in almost every modern enterprise. The combination of these factors actualizes the problem associated with ensuring the information security of the enterprise. The purpose of the current article is to consider the key issues regarding the risk-based audit of information security in the context of comprehensive information security. The scientific significance of the work consists in the possibility of using the presented materials to form strategies for ensuring information security of modern enterprises.

Keywords: Information, information security, audit, risk-based approach, information protection.

Повсеместный перевод информационных активов, денежных средств и коммуникаций в электронную форму создает новый тип актива – информацию. Информация также, как и любая другая ценность, подвержена атакам и нарушениям целостности со стороны хакеров и мошенников. На сегодняшний день актуализируется возникновение рисков в области обеспечения защиты информации. При этом основные угрозы описаны в Доктрине государственной информационной безопасности (далее – ИБ). Необходимо отметить, что

игнорирование угроз неизбежно приводит к нарушению целостности информационной инфраструктуры предприятий и снижению их конкурентоспособности на рынке [1].

Вопрос актуальности информационной безопасности требует детального отношения к вопросам ее защиты. В начале своего пути обеспечение защиты информации решалось на основе использования криптографических алгоритмов шифрования, установки межсетевых экранов и иных средств разграничения доступа. Однако в современных условиях всего этого недостаточно. Так как любой информационный актив подвергается все более сложным и усовершенствованным атакам со стороны злоумышленников. Вместе с этим, остается угроза перехвата управления критическими объектами информационной инфраструктуры.

Статистические сведения свидетельствуют о непрерывном повышении инцидентов ИБ на 5% каждые полгода. Также проблемой становится и то, что вместе с ростом преступлений в области компьютерной безопасности снижается и раскрываемость. На сегодняшний день раскрываемость инцидентов информационной безопасности в современных организациях не превышает 41 процента.

На сегодняшний лень выделяется несколько основных и в то же время наиболее опасных угроз информационной безопасности. В их числе находится кража информационных активов, вредоносные программы, мошенничество и иные угрозы. На Рисунке 1 представлена статистика, отражающая процентное соотношение реализации в зависимости от угроз [2].

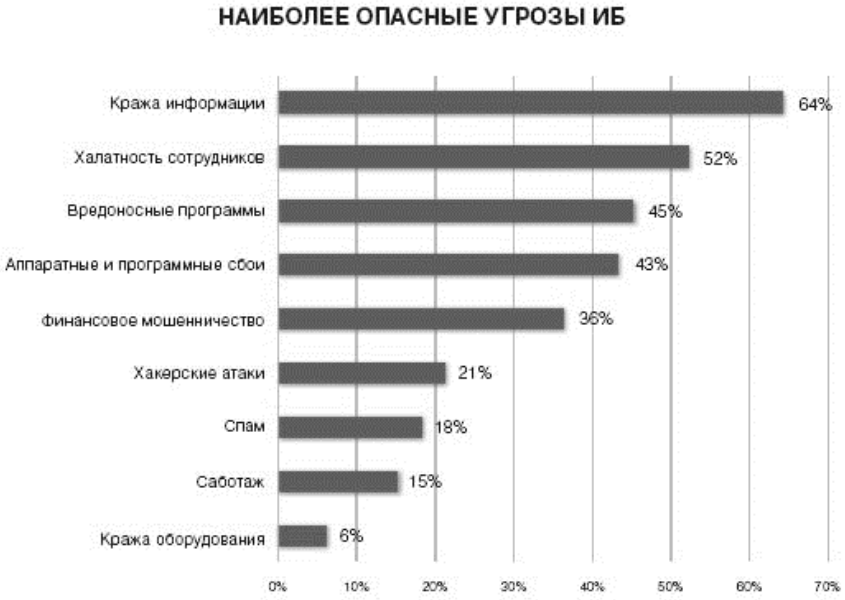

Рисунок 1 – Рейтинг наиболее опасных угроз ИБ

Актуальность информационной безопасности подтверждается рядом основных факторов, которые выделяются современными компаниями в результате их функционирования. Первым из них является то, что практически у всех современных компаний имеются ресурсы ограниченного доступа, нуждающиеся в защите. Предприятия, больницы и правительства подвержены риску, поскольку они обрабатывают огромные объемы конфиденциальной информации. Это включает в себя финансовые счета, номера социального страхования, медицинскую информацию, секреты национальной безопасности и многое

другое. Отдельные люди тоже не застрахованы. Если на предприятии имеется какая-либо информация о системе (пароли к банковским счетам, социальному обеспечению, веб-сайтам розничной торговли и так далее), то она является уязвимой.

На сегодняшний момент времени происходит активное развитие, создание новых и улучшение существующих методов защиты информации. Вместе с разработкой аппаратно-программных инструментов активное развитие получают и различные методологические, организационные и правовые аспекты защиты информации. Одним из наиболее актуальных и показывающих эффективные результаты своего использования инструментом является аудит информационной безопасности организации.

Аудит информационной безопасности - это процесс оценки и проверки системы защиты информации в организации. Аудит проводится с целью выявления нарушений безопасности, оценки уровня риска и уязвимостей, а также определения необходимых мер для улучшения безопасности. Аудит может быть проведен как внутренними специалистами, так и сторонними экспертами. Результаты аудита используются для разработки плана мер по улучшению безопасности, обучения персонала, а также для улучшения процессов управления информационной безопасностью в организации [3].

На Рисунке 2 представлены ключевые задачи, решаемые в рамках проведения аудита информационной безопасности каждой отдельной организации. В составе данных задач должен быть включен полный комплекс анализа рисков и угроз, а также формирования требований к защите информации.

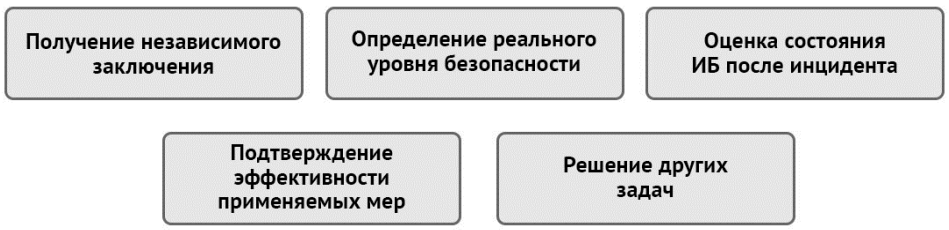

Рисунок 2 – Основные задачи проведения аудита информационной безопасности

Аудит информационной безопасности включает в себя проверку и оценку системы безопасности информации, включая:

- Оценку степени угрозы для информационной системы
- Проверку соответствия политикам и правилам безопасности информации
- Анализ доступа к информации и правильности настроек безопасности
- Проверку защиты от несанкционированного доступа
- Оценку устойчивости и надежности информационной системы при возникновении различных ситуаций
- Проверку соответствия законодательству и стандартам в области информационной безопасности.

В результате аудита информационной безопасности может быть выявлены недостатки и уязвимости системы безопасности, а также рекомендации по улучшению защиты информации. Так, результатом аудита информационной безопасности является отчет, где описывается:

- Состояние системы информационной безопасности и ее риски;
- Наличие и эффективность мер защиты от угроз;
- Уровень управления безопасностью информации в организации;
- Рекомендации по усовершенствованию системы информационной безопасности.

Такой анализ поможет организациям определить слабые точки в защите информации и разработать планы по их устранению, повышению уровня информационной безопасности и уменьшению рисков.

Стандартами для проведения данного аудита ИБ являются ISO 27001, PCI DSS, 17 приказ ФСТЭК и иные. При этом каждой из представленных на рис. 9 вариантов может производиться как отдельно, так и в комплексе. Это зависит от целей проведения аудита и ресурсов той или иной организации. Сам аудитор также может применять различные методы, включая имитацию атак без реального повреждения информационной инфраструктуры. Имитацией атак проверяются такие факторы, как: наличие уязвимостей аппаратно-программной части организации; устойчивость сети на несанкционированный доступ к информации; оперативность реагирования системы на сбои; возможность проникновения в структуру и иное [4].

Одним из наиболее актуальных и показывающих эффективные результаты своего проведения является комплексный аудит информационной безопасности. Комплексный аудит ИБ включает в себя исследование текущего состояния системы информационной безопасности организации для получения объективной оценки относительно уровня ее защиты. Помимо этого, по результатам проведения аудита производится разработка рекомендаций совершенствования системы информационной безопасности.

Основными преимуществами проведения комплексного аудита ИБ является получение наиболее полной, объективной и в то же время независимой оценки состояния информационной инфраструктуры. Фактически говоря, комплексный аудит ИБ является симбиозом всех видов аудита информационной безопасности. Именно по результатам его проведения заказчик может получить оценку уровня и состояния существующей системы информационной безопасности, а также защищенность внутренних и внешних информационных ресурсов.

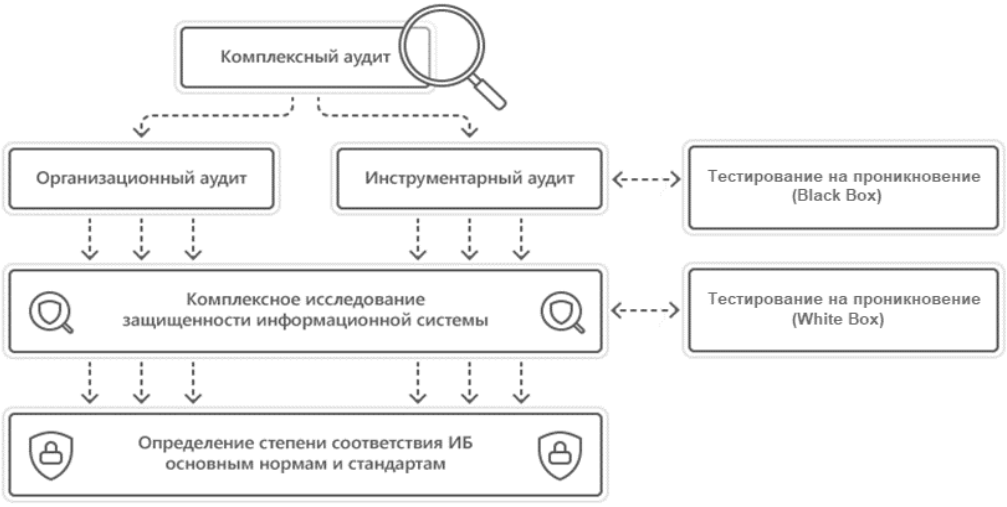

Рисунок 3 – Направления при проведении комплексного аудита ИБ

Вместе с этим, рассматриваемый метод проведения аудита также основывается на стандартах информационной безопасности. Определение угроз и рисков ИБ основывается на нормах и стандартах. На Рисунке 3 представлен состав мероприятий при проведении комплексного аудита информационной безопасности.

В общем виде комплексный аудит имеет в своем составе и такие виды аудита, как: экспертный аудит; тестирование на проникновение; аудит Web-безопасности; аудит информационных систем. Также важно отметить, что состав работ в рамках его проведения заранее обсуждается и утверждается с заказчиком. Провести данный вид аудита можно как внешними, так и внутренними силами специалистов в организации. Однако во втором случае не всегда наблюдается объективная оценка уровня защиты информационных систем. Именно поэтому для получения всесторонне объективной оценки прибегают к использованию внешних экспертов [5].

На Рисунке 4 представлен один из алгоритмов, отражающих основных этапы проведения комплексного аудита ИБ на основе риск-ориентированного подхода:

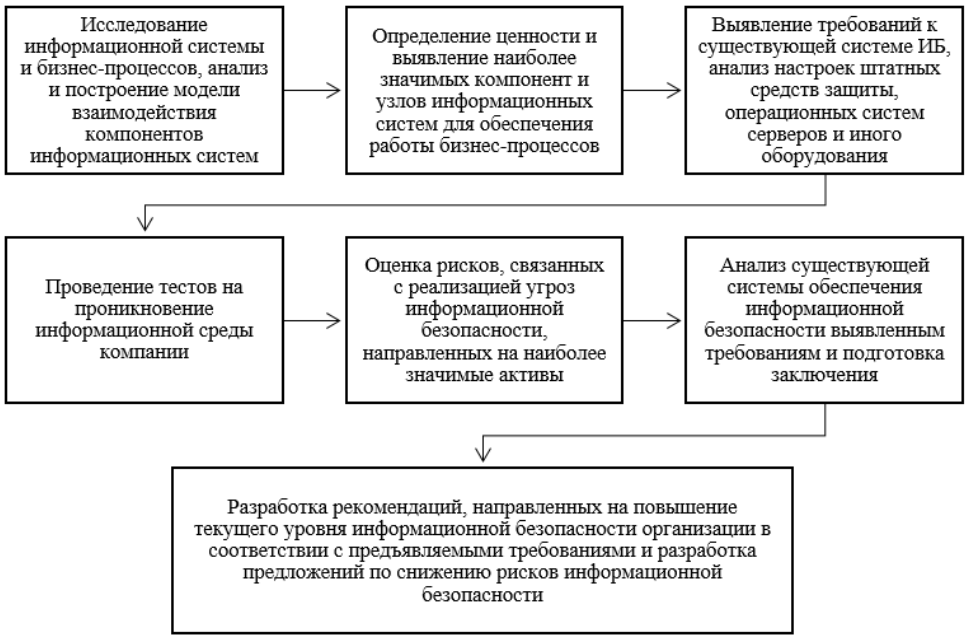

Рисунок 4 – Алгоритм проведения комплексного аудита ИБ

В результате проведения данного вида аудита организация получает детализированный отчет, в котором отражается информация о каждом выявленном недочете, уязвимостях и слабых местах в информационной инфраструктуре. Именно этот отчет является основой в формировании рекомендаций по доработке и улучшению уровня ИБ организации.

Риск-ориентированный подход к аудиту ИБ – это метод, основанный на идентификации, оценке, контроле и управлении рисками, связанными с безопасностью информационных систем. Данный подход подразумевает наличие систематических процедур, инструментов и методов, которые помогают анализировать и оценивать риски в ИБ на стадии планирования, реализации и эксплуатации. Риск-ориентированный подход позволяет выявлять уязвимости и

определять наиболее значимые угрозы, которые могут нарушить безопасность информационной системы, а также определять эффективность контрольных мер, которые применяются для управления рисками безопасности информации. Основным принципом данного подхода является максимальная ориентация на защиту самых ценных активов организации и сокращение рисков до приемлемого уровня. Таким образом, риск-ориентированный подход к аудиту ИБ помогает улучшить уровень безопасности информационных систем организации и значительно снизить вероятность негативных последствий нарушения безопасности.

Проведение аудита ИБ на основе риск-ориентированного подхода включает в себя пять основных действий, в составе каждого из которых можно выделить конкретное действие, значение и результат. Далее представлен каждый из этапов проведения данного аудита.

- **Этап 1.** Проведение анализа бизнес-процессов;
- **Этап 2.** Проведение оценки рисков;
- **Этап 3.** Определение и внедрение необходимых средств контроля;
- **Этап 4.** Тестирование, проверка и отчет;
- **Этап 5**. Непрерывный мониторинг и управление.

Таким образом, основной целью представленной статьи являлось выполнение анализа по вопросу проведения риск-ориентированного аудита информационной безопасности в контексте комплексного обеспечения защиты информации. Подход к программе кибербезопасности, основанный на оценке рисков, а не на соответствии или контрольных списков, принесет много преимуществ, включая персонализированную оценку риска, расставленные по приоритетам пробелы, адаптированные средства контроля и более надежный цикл для устранения новых рисков и уязвимостей.

Также в заключение стоит отметить, что аудит ИБ на основе риск-ориентированного подхода предоставляет руководителям современных организаций получить независимый взгляд на существующую систему ИБ и выявить шаги, необходимые для совершенствования системы информационной безопасности. Данный аудит дает оценку защищенности компании, выявляет риски и создает план конкретных действий, направленных на минимизацию их влияния.

Список литературы

1. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018.
2. Двойнишников Н.Э., Исламутдинова Д.Ф. Понятие и сущность аудита безопасности информационных систем // Московский экономический журнал. 2019.
3. Букалерова Л.А., Лапшин В.Ф., Остроушко А.В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник СурГУ. 2021.
4. Макарейко Н.В. Риск-ориентированный подход при осуществлении контроля и надзора // Юридическая техника. 2019.

5. Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019.

References

1. Makarenko S.I. Audit of information security: main stages, conceptual foundations, classification of measures // Control Systems, Communications and Security. 2018.
2. Dvoynishnikov N.E., Islamutdinova D.F. The concept and essence of the audit of the security of information systems. Moscow Economic Journal. 2019.
3. Bukalerova L.A., Lapshin V.F., Ostroushko A.V. Risk-oriented approach in the field of legal regulation of information security of minors // Vestnik SurGU. 2021.
4. Makareiko N.V. Risk-oriented approach in the implementation of control and supervision // Legal Technique. 2019.
5. Maslova M.A. Analysis and identification of information security risks // Scientific result. Information Technology. 2019.