УДК 004.056

П.А. Фильченков
Белорусский государственный университет информатики и радиоэлектроники
Минск, Беларусь

МЕТОДЫ И СРЕДСТВА АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. *В статье представлено обоснование важности и актуальности вопросов в сфере информационной безопасности Приведено определение аудита безопасности информационных систем, дано обоснование его важность на современном этапе развития экономики нашего государства.*

P.A. Filchenkov
Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus

SECURITY AUDIT OF INFORMATION SYSTEMS

Abstract. *The article presents the justification of the importance and relevance of issues in the field of information security the definition of information systems security audit is given, the justification of its importance at the present stage of economic development of our state is given.*

В настоящее время в организациях уделяется большое внимание вопросам информационной безопасности. Эти вопросы связаны с установлением порядка реализации комплекса мер организационного и технического характера, направленных на обеспечение конфиденциальности, целостности, доступности, подлинности и сохранности информации, а также на защиту информационных систем. Неотъемлемой составляющей этого комплекса мер является проведение на регулярной основе аудита информационной безопасности. Аудит информационной безопасности является важнейшим компонентом непрерывного цикла процессов управления безопасностью информации в организации [1]. Одно из направлений этого процесса – это аудит безопасности информационных систем. Важность развития этого направления обусловлена тем, что в настоящее время с помощью информационных систем обрабатывается информация, распространение и / или предоставление которой ограничено (персональные данные, служебная информация ограниченного распространения, коммерческая тайна).

Цель работы состояла в обосновании актуального комплекса методов и средств проведения аудита безопасности информационных систем.

Для достижения поставленной цели были решены следующие задачи:

– систематизировать виды аудита безопасности информационных систем и перечень задач, которые должны решаться в ходе реализации этого процесса;

– определить основные технические нормативные правовые акты, с учетом которых должен проводиться аудит безопасности информационных систем в Республике Беларусь.

Основные виды аудита безопасности информационных систем представлены на рис. 1 [1].

Вопросы аудита безопасности информационных систем на основе анализа и управления безопасности информации рассмотрены в работах отечественных и зарубежных авторов: А. Ю. Азаров, В. В. Анищенко, В. А. Бойправ, Д. Лебланк, С. А. Петренко, В. Столингс, Л. Л. Утин, М. Ховард, Б. Шнайер и др. По результатам анализ работ [2–4], что основными задачи аудита безопасности информационных систем являются следующие:

– обнаружение текущих проблем и уязвимостей в структуре информационной системы;

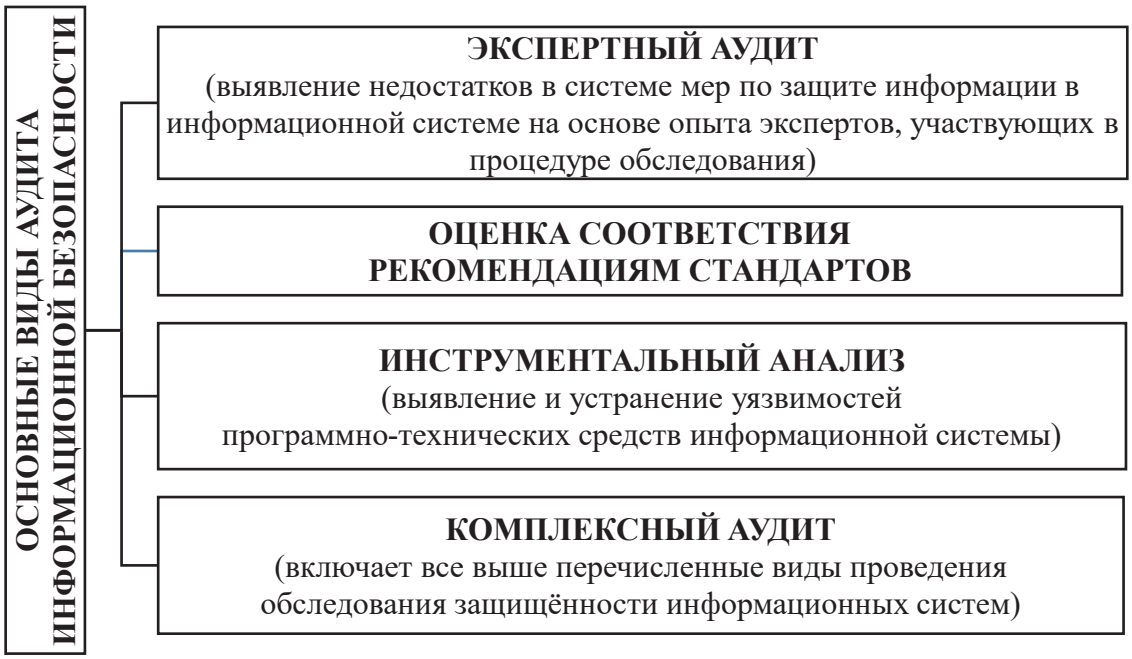

Рис. 1 - Основные виды аудита безопасности информационных систем

– выявление потенциальных уязвимостей в информационной системе для оценки и контроля потенциальных рисков;

– получение полной картины о состоянии структуры информационной системы организации для ее контроля и оптимизации бюджета;

– оценка системы защиты информации на соответствие требованиям Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

– проведение подготовки к внедрению структурированной политики информационной безопасности.

Ниже представлен перечень технических нормативных правовых актов, с учетом которых должен проводиться аудит безопасности информационных систем в Республике Беларусь, а также результаты проведенного анализа содержания этих документов.

1. Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» – регулирует общественные отношения, возникающие при: поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией; создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов; организации и обеспечении защиты информации.

2. Закон Республики Беларусь от 28.12.2009 № 113-З «Об электронной цифровой подписи» – направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

3. Закон от 07.05.2021 № 99-З Республики Беларусь «О защите персональных данных» – направлен на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных.

4. Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 (в ред. Указа Президента Республики Беларусь от 9 декабря 2019

г. № 449) «О некоторых мерах по совершенствованию защиты информации» – в целях совершенствования технической и криптографической защиты информации были утверждены некоторые нормативно-правовые акты в сфере информационной безопасности.

5. Концепция информационной безопасности Республики Беларусь, утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 – обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, конструктивного взаимодействия, повышения эффективности защиты национальных интересов в информационной сфере.

6. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» – утверждает следующие Положения:

– о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

– о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

– о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации;

– о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации;

– о порядке ведения Государственного реестра критически важных объектов информатизации.

7. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь» – утверждает показатели уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности.

8. СТБ ISO/IEC 27001-2011 «Информационные технологии.

Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования» – в настоящем стандарте устанавливаются требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию документально оформленной системы менеджмента информационной безопасности в контексте общих бизнес-рисков организации.

9 СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» – настоящий стандарт идентичен международному стандарту ИСО/МЭК 27002:2005 «Информационная технология. Методы и средства обеспечения безопасности.

Таким образом, аудит безопасности информационных систем должен состоять в оценке состояния как программно-технических средств информационной системы, так и системы защиты информации в соответствии с представленными выше техническими нормативными правовыми актами.

Список использованных источников

1. Грекул, В. И. Аудит информационных технологий: учебник для вузов / В. И. Грекул // М.: Горячая линия – Телеком, 2020. – 154 с.

2. Бойправ, В. А. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. 2022; 19(4): 42–52.

3. Бойправ, В. А. Программное средство для проведения аудита системы защиты информации организации / В. А. Бойправ, В. В. Ковалев, Л. Л. Утин // Доклады БГУИР. – 2018. – № 5(115). – С. 44–49.

4. Information security risk assessment / I. Kuzminykh [et. al.] // Encyclopedia. – 2021. – Vol. 1(3). – P. 602–617.

УДК 338.1

Н.И. Белодед, Е.С. Хорошун
Академия управления при Президенте Республики Беларусь,
Минск, Беларусь

ЭКОНОМИКА ДАННЫХ: ОТ BIG DATA К ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ

***Аннотация**. В статье рассматривается роль больших данных и искусственного интеллекта в современной экономике. Кроме того, обсуждаются важность и влияние больших данных на принятие стратегических решений*