УДК 004.056

ПОДХОДЫ ДЛЯ ПРОВЕДЕНИЯ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ

П.А. Фильченков, магистрант,
О.В. Бойправ, канд. техн. наук, доц.
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь

Приведены цели, задачи и формы проведения аудита безопасности информационных систем учреждений здравоохранения. Рассматриваются теоретические и практические подходы к проведению аудита безопасности информационных систем учреждений здравоохранения.

Ключевые слова: *аудит безопасности, информационные системы, учреждения здравоохранения, информационная безопасность, оценка рисков.*

Под аудитом безопасности информационных систем (ИС) учреждений здравоохранения понимается проверка таких систем на соответствие требованиям нормативных правовых актов и стандартам в сфере защиты информации, с последующей оценкой рисков информационной безопасности, характерных для таких систем. В [1] представлены результаты анализа особенностей информационных систем учреждений здравоохранения Республики Беларусь. В [2] приведены критерии для выбора и разработки средств аудита безопасности информационных систем учреждений здравоохранения с учетом результатов анализа, представленных в [1]. Средства, приведенные в [2], необходимо использовать для достижения целей аудита (рисунок 1).

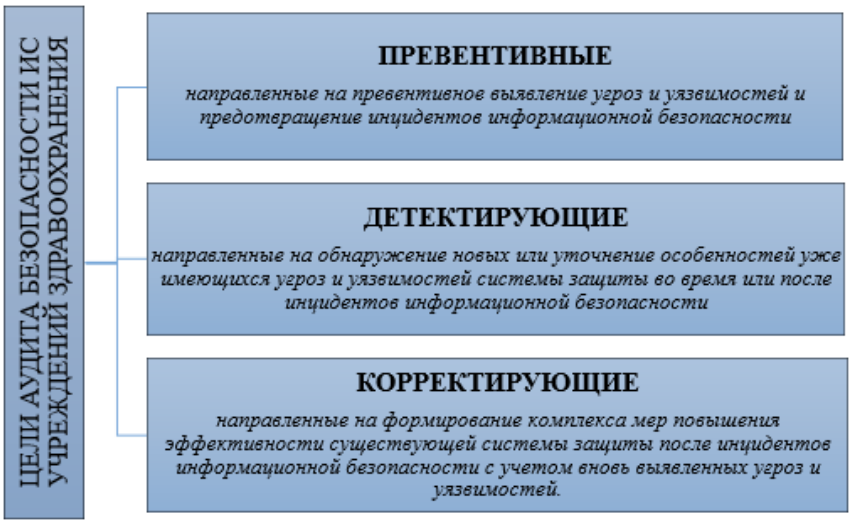

Рисунок 1. – Цели аудита безопасности информационных систем учреждений здравоохранения

Процесс достижения целей аудита с использованием соответствующих средств состоит в решении общей и частных задачи аудита [3–7]. Проверка и оценивание ИС

учреждений здравоохранения на соответствие критериям, которые определяют требования к уровню информационной безопасности (ИБ), – это общая задача аудита безопасности ИС учреждений здравоохранения. К частным задачам аудита безопасности ИС учреждений здравоохранения можно отнести следующие:

– анализ рисков, связанных с возможностью реализации угроз безопасности;

– оценка текущего уровня защищенности;

– выявление уязвимостей в подсистеме защиты и «узких мест» ИС учреждений здравоохранения; оценка соответствия ИС учреждений здравоохранения и ее защиты существующим стандартам в области ИБ, а также политике безопасности учреждений здравоохранения;

– разработка рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты учреждений здравоохранения.

Можно выделить следующие формы проведения аудита безопасности ИС учреждений здравоохранения в зависимости от типа частной задачи, решаемой в рамках этого процесса:

– организационно-нормативный аудит (анализируется организационные мероприятия обеспечения ИБ учреждений здравоохранения и нормативные акты по этому вопросу);

– технический аудит (анализируется технические средства и способы обеспечения ИБ учреждений здравоохранения).

На рисунке 2 представлены процедуры, которые должны быть реализованы в ходе проведения аудита безопасности ИС учреждений здравоохранения.

Рисунок 2. – Процедуры, которые должны быть реализованы в ходе проведения аудита безопасности информационных систем учреждений здравоохранения

В модель аудита безопасности ИС учреждений здравоохранения входят цели, объект, требования, порядок проведения, исполнители, теоретические и практические подходы, масштаб и глубина.

Для описания модели нарушителя/противника необходимы: 1) формализованное понятие нарушителя/противника; 2) критерии нарушения информационной безопасности ИС; 3) категорирование нарушителей/противников; 4) предположения о квалификации, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории нарушителей/противников; 5) предположения о сценариях действий каждой категории нарушителей/противников; 6) уровень полномочий и способы получения доступа к системе для каждой категории нарушителей/противников [4].

Модель угроз должна включать в себя описание категорий и групп угроз

Выделяют следующие категории угроз:

– угрозы конфиденциальности;

– угрозы доступности;

– угрозы целостности;

– угрозы подлинности;

– угрозы сохранности.

Выделяют следующие группы угроз:

– угрозы, реализуемые путем использования технических каналов утечки информации;

– угрозы, реализуемые с использованием средств и способов информационно-технических воздействий;

– угрозы, реализуемые с использованием средств и способов информационно-психологических воздействий или социальной инженерии) [3].

К общим практическим подходам к проведению аудита безопасности ИС учреждений здравоохранения относятся: 1) аудит на основе анализа рисков; 2) аудит на основе анализа стандартов информационной безопасности; 3) аудит на основе комбинирования анализа рисков и анализа стандартов информационной безопасности; 4) аудит на основе экспериментальных исследований системы или ее прототипа. Аудит на основе анализа рисков является достаточно трудоемким и для его проведения необходимо, чтобы аудитор был высоко квалифицированным. Аудит на основе анализа стандартов информационной безопасности – самый практичный. Аудитор в этом случае должен правильно определить перечень требований стандарта, соответствие которым требуется обеспечить для конкретной исследуемой ИС. Если нужен эффективный подход к проведению аудита, то в таком случае стоит применять комбинирование двух вышеописанных видов аудита. Аудит на основе экспериментальных исследований ИС учреждения здравоохранения осуществляется при использовании против ИС средств или способов информационно-технических и информационно-психологических воздействий для того, чтобы на практике проверить эффективность технических и/или организационных мер защиты.

К основным теоретическим подходам к проведению аудита безопасности ИС учреждений здравоохранения относятся: 1) процессный подход; 2) подходы, основанные на модели оценки; 3) подходы, основанные на модели зрелости. Процессный подход позволяет представить деятельность по обеспечению ИБ, как вспомогательный процесс в функционировании учреждения здравоохранения.

На рисунке 3 представлена иерархия процессов деятельности учреждения здравоохранения.

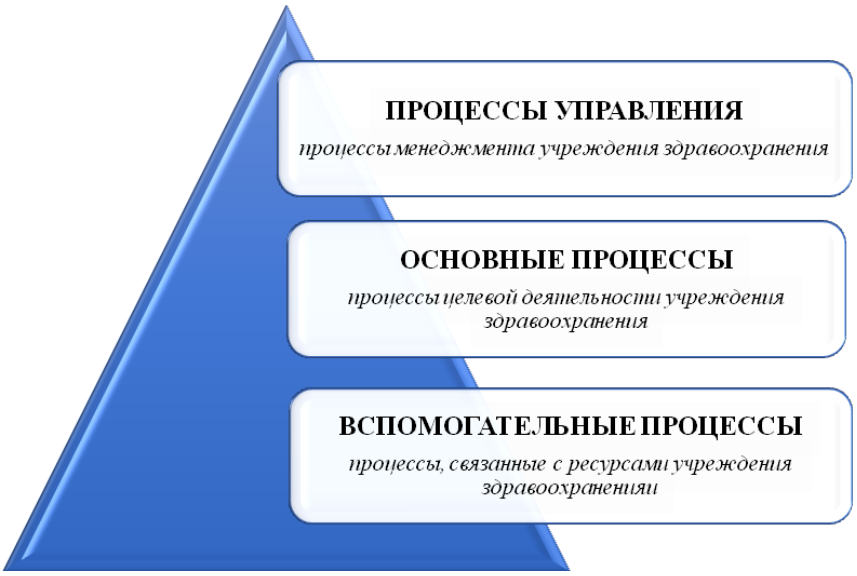

Рисунок 3. – Иерархия процессов деятельности учреждения здравоохранения

В теоретическом подходе к проведению аудита безопасности ИС учреждений здравоохранения, основанном на модели оценки, определяется перечень, модель оцениваемых процессов, совокупность показателей, используемых для сбора данных и определения степени достижения установленных критериев обеспечения ИБ ИС.

На рисунке 4 показана схема уровней зрелости процессов учреждения здравоохранения от первого до пятого, которая учитывается в теоретической модели, основанный на модели зрелости.

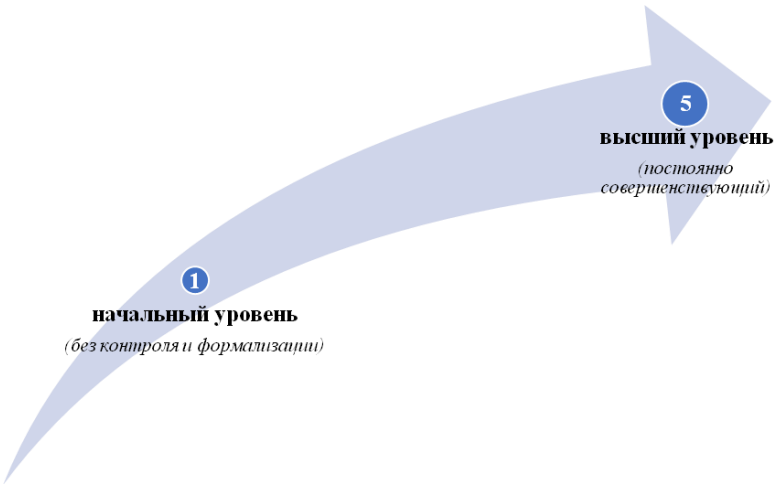

Рисунок 4. – Схема уровней зрелости процессов учреждения здравоохранения от первого до пятого

Таким образом, аудит безопасности ИС учреждений здравоохранения должен состоять в анализе нормативных правовых актов (в том числе локальных) в сфере защиты информации, последовательном проведении тестирования подсистем указанных ИС, а также анализе реализуемых в рамках них процессов.

ЛИТЕРАТУРА

1. Фильченков, П. А. Анализ особенностей информационных систем учреждений здравоохранения Республики Беларусь / П. А. Фильченков // Управление информационными ресурсами : Материалы XX Междунар. науч.-практич. конф., Минск, 29 марта 2024 года. – Минск : Академия управления при Президенте Республики Беларусь, 2024. – С. 314–315.
2. Фильченков, П. А. Критерии для выбора и разработки средств аудита безопасности информационных систем учреждений здравоохранения / П. А. Фильченков // Технические средства защиты информации : тез. докл. XXII Белорусско-Российской науч.-техн. конф. (Республика Беларусь, Минск, 12 июня 2024 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2024. – С. 92–93.
3. Аудит информационной безопасности органов исполнительной власти: учеб. пособие / В. И. Аверичников [и др.] – М.: Флинта, 2011. – 100 с.
4. Макаренко, С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С. И. Макаренко // Системы управления, связи и безопасности. – 2018. – № 1. С. 1–29.
5. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов ; под ред. А.С. Маркова. – М.: Радио и связь, 2012. – 192 с.
6. Астахов, А. Введение в аудит информационной безопасности / А. Астахов // GlobalTrust Solutions [Электронный ресурс]. – 2018. – Режим доступа: http://globaltrust.ru.– Дата доступа: 29.10.2024.
7. Мониторинг и аудит информационной безопасности автоматизированных систем / В. В. Кульба – М.: ИПУ им. В.А. Трапезникова РАН, 2009. – 94 с.