Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:005.71

КЛИМОВИЧ
Артур Юрьевич

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЙ

Автореферат
на соискание степени магистра
по специальности 1–98 80 01 Информационная безопасность

_____

Научный руководитель
канд. техн. н., доцент
БЕЛОУСОВА Елена Сергеевна

_____

Минск 2023

ВВЕДЕНИЕ

Многие государственные организации имеют дело с информацией ограниченного распространения, и защита такой информации является одной из важнейших задач обеспечения информационной безопасности. Так как аудит информационной безопасности (ИБ) позволяет получить представление о состоянии защищенности информационной системы, то разработка единой методики проведения аудита ИБ позволит в целом повысить эффективность контроля за ИБ в государственных организациях.

Вопрос организации безопасного функционирования корпоративных информационных систем организаций любого уровня на протяжении ряда последних лет является актуальным. Накопленные к настоящему времени теоретические разработки и практический опыт по защите отдельных компонентов информационных систем являются достаточными для обеспечения стабильной работы информационных систем, однако на практике довольно часто возникает необходимость оценить адекватность принятых мер по обеспечению информационной безопасности существующим угрозам.

Целью диссертационной работы является совершенствование методики проведения внутреннего аудита информационной безопасности государственных организаций.

Для достижения поставленной цели в диссертации необходимо решить следующие задачи:

1 Изучить действующие международные и государственные стандарты в области проведения аудита ИБ с целью совершенствования методики проведения внутреннего аудита ИБ.

2 Изучить методику проведения внутреннего аудита информационной безопасности, применяемой в организации в настоящее время, проанализировать отчеты о результатах проведения внутреннего аудита ИБ.

3 Провести количественную оценку рисков информационной безопасности для структурного подразделения организации.

4 Совершенствовать методику проведения внутреннего аудита информационной безопасности и провести ее апробацию в выбранном структурном подразделении организации.

Совершенствование методики проведения внутреннего аудита информационной безопасности позволит повысить эффективность контроля за состоянием информационной системы организации, что поможет сохранить доступность, целостность и конфиденциальность информационных активов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «*Обеспечение безопасности*

человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является совершенствование методики проведения внутреннего аудита информационной безопасности государственных организаций.

Для достижения поставленной цели в диссертации необходимо решить следующие задачи:

1 Изучить действующие международные и государственные стандарты в области проведения аудита ИБ с целью совершенствования методики проведения внутреннего аудита ИБ.

2 Изучить методику проведения внутреннего аудита информационной безопасности, применяемой в организации в настоящее время, проанализировать отчеты о результатах проведения внутреннего аудита ИБ.

3 Провести количественную оценку рисков информационной безопасности для структурного подразделения организации.

4 Совершенствовать методику проведения внутреннего аудита информационной безопасности и провести ее апробацию в выбранном структурном подразделении организации.

Личный вклад соискателя ученой степени

Личный вклад автора заключается в оценке актуальных угроз для конкретной информационной системы, разработке методики проведения внутреннего аудита ИБ, основанной на оценке рисков для Государственного комитета судебных экспертиз Республики Беларусь, и последующей оценке эффективности разработанной методики в процессе проведения аудита ИБ в одном из территориальных подразделений организации.

Определение целей и задач исследований, разработка методики проведения аудита информационной безопасности и формулировка практических рекомендаций по ее применению проводились совместно с научным руководителем, кандидатом технических наук, доцентом Е.С. Белоусовой.

Апробация диссертации и информация об использовании ее результатов

Результаты диссертационной работы приняты к использованию подразделением по обеспечению ТЗИ Центрального аппарата Государственного комитета судебных экспертиз Республики Беларусь и прошли апробацию при проведении аудита информационной безопасности в Управлении Государственного комитета судебных экспертиз по Могилевской области. Сведения, полученные в результате проведения аудита по разработанной методике, были использованы для формирования плана по

усилению мер по технической защите информации в Государственном комитете судебных экспертиз Республики Беларусь.

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 печатная работа, в том числе 1 статья и тезис в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из общей характеристики работы, перечня условных обозначений, введения, трех глав с выводами по каждой главе, заключения, библиографического списка, 1 приложения.

Общий объем диссертационной работы составляет 64 страниц, из них 48 страниц текста, 4 рисунка на 2 страницах, 6 таблиц на 6 страницах, список использованных библиографических источников (19 наименований) и список публикаций автора по теме диссертации (1 наименование) на 2 страницах, 1 приложение на 1 странице, графический материал на 5 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Климовича А.Ю. «Методика проведения аудита информационной безопасности в государственной организации» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 22.05.2023 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 86,22 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрены проблемы обеспечения информационной безопасности в государственных организациях, в информационной системе которых обрабатывается информация ограниченного распространения, обозначена роль аудита ИБ как средства, позволяющего получить представление о состоянии защищенности информационной системы. Поставлена цель совершенствования методики проведения аудита ИБ для повышения эффективности контроля за ИБ в государственной организации.

В **общей характеристике работы** показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе изучены цели и задачи аудита информационной безопасности, основные международные стандарты, определяющие подходы к проведению аудитов ИБ (в их числе серия международных стандартов ISO/IEC 27001 и их российский аналог ГОСТ Р ИСО/МЭК 27001-2021, стандарт ISO 27005, руководящие документы ФСТЭК, стандарт COBIT,

специальные публикации института NIST SP 800-ой серии и рекомендации по внедрению ИБ CIS Controls). На их основе можно сделать вывод о том, что для эффективного обеспечения информационной безопасности в организации аудит ИБ должен включать в себя проверку состояния физической безопасности информационной инфраструктуры, техническое обследование информационных систем – программных и аппаратных средств, а также анализ имеющихся политик информационной безопасности и другой организационной документации. По его результатам можно будет оценить эффективность вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности. Также рассмотрен порядок проведения внутреннего аудита информационной безопасности, применяемый в организации в настоящее время.

Во второй главе описана структура организации и особенности расположения элементов информационной системы в ее Центральном аппарате и территориальных органах. Были определены категории информации, обрабатываемой в ИС организации, активы, входящие в состав ИС, а также описан состав системы защиты информации, функционирующей в организации. В ходе сбора и анализа материалов, предоставленных подразделением, отвечающим за техническую защиту информации, были рассмотрены отчеты о вирусной активности, собранные средствами антивирусной защиты, отчеты об инцидентах информационной безопасности, и отчеты о результатах аудита ИБ, проведенного в организации в период с 2018 по 2022 годы. Проведен анализ рисков информационной безопасности, характерных для информационной системы организации. Были описаны наиболее вероятные угрозы, и проведена оценка их актуальности. Проведена процедура количественной оценки рисков, на основе которой для каждого ценного актива были выявлены актуальные угрозы и вероятности их реализации. Полученные в конечном счете значения величин рисков позволяют определить, какие риски можно считать приемлемыми, а какие необходимо подвергнуть дальнейшей обработке с целью минимизации.

Финальное значение оценки риска может принимать значения от 1 до 150, при этом чем выше значение оценки риска, тем сильнее актив информационной системы подвержен воздействию конкретной угрозы и тем больший ущерб может быть нанесен в случае реализации угрозы.

Приемлемым риском считается риск, чье числовое значение находится в промежутке от 1 до 50, такой риск считается незначительным, и обработка такого риска не требуется.

Средний риск, числовое значение которого находится в диапазоне от 51 до 100 рекомендован к обработке с целью его минимизации. К средним рискам были отнесены:

– реализация угрозы «воздействие вредоносного ПО» в отношении актива «ПЭВМ сотрудников» (значение риска 72);

– реализация угрозы «несанкционированное получение доступа к сети Интернет» в отношении актива «ПЭВМ сотрудников» (значение риска 72);

– реализация угрозы «воздействие вредоносного ПО» в отношении актива «Сервера баз данных» (значение риска 80);

– реализация угрозы «воздействие вредоносного ПО» в отношении актива «Файловые сервера» (значение риска 80).

Высокий риск, чье числовое значение находится в диапазоне от 101 до 150, считается существенным, и его обработка обязательна. К высоким рискам относятся:

– реализация угрозы «утечка информации ограниченного распространения» в отношении актива «Файловые сервера» (значение 105);

– реализация угрозы «утечка информации ограниченного распространения» в отношении актива «Сервера баз данных» (значение 105).

В третьей главе сформулирована методика проведения внутреннего аудита информационной безопасности в государственной организации. Разработанная методика заключается в изучении информационной системы организации и выявлении наиболее актуальных угроз информационной безопасности. Методика проведения аудита информационной безопасности на основе оценки рисков включает следующие этапы:

1 Определение области аудита. В этом этапе определяются подразделения, в отношении которых будет проводится аудит, составляется список.

2 Идентификация угроз и уязвимостей. На этом этапе производится анализ угроз и уязвимостей информационной системы проверяемых подразделений с целью выявления актуальных угроз информационной безопасности, которые могут возникнуть в процессе ее функционирования.

3 Оценка рисков. В этом этапе проводится оценка вероятности наступления угроз и их возможного воздействия на информационную систему и ее активы. Для этого используются количественные методы оценки рисков, в зависимости от специфики деятельности конкретных подразделений.

4 Оценка соответствия системы требованиям безопасности. На этом этапе производится:

– анализ соответствия информационной системы требованиям нормативно-правовых актов, политик безопасности, стандартов и других регуляторных документов, действующих в организации;

– анализ процедур контроля доступа к данным в информационной системе, проверка разграничения прав пользователей ИС;

– проверка безопасности сети (проводится анализ безопасности сетевой инфраструктуры, проверка настроек активного сетевого оборудования);

5 Оценка физической безопасности. В этом этапе производится анализ мер физической защиты информационной системы, таких как защита серверных комнат, серверов и другого оборудования.

6 Подготовка отчета. На этом этапе подводятся итоги аудита, формируется отчет, в котором описываются выявленные уязвимости и риски, а также рекомендации по улучшению безопасности информационной системы. Результаты в виде отчета направляются в адрес руководителя проверяемого

подразделения, и сотрудникам, ответственным за техническую защиту информации.

На основе описанных во второй главе диссертации величины рисков, характерных для Управления Государственного комитета судебных экспертиз Республики Беларусь по Могилевской области, были определены наиболее высокие риски – реализация угроз воздействия на ПЭВМ сотрудников организации вредоносного ПО и получение несанкционированного доступа к сети Интернет (средние риски), а также реализация воздействия вредоносного ПО и утечка информации ограниченного распространения, затрагивающее сервера баз данных и файловые сервера организации (высокие риски). Для минимизации этих рисков было предложено использовать дополнительные меры обеспечения информационной безопасности. К дополнительным организационным мероприятиям были отнесены:

– анализ инцидентов информационной безопасности управлений Государственного комитета по областям и г. Минску для выявления аномальных и опасных инцидентов ИБ;

– анализ существующих схем сегментов сетей передачи данных для оценки возможных уязвимостей;

– контроль за выполнением работ по переводу информационного обмена между центральным аппаратом и территориальными управлениями на защищенные каналы электросвязи;

– осуществление контроля порядка выдачи логинов и паролей для доступа к базам МВД в территориальных органах организации;

– осуществление контроля наличия, порядка хранения, регистрации и содержания информации на съемных носителях цифровой информации, предназначенных для работы со служебной информацией ограниченного распространения;

– проведение ревизии правовых актов организации в области технической защиты информации, при необходимости внесение изменений и дополнений, разработка новых НПА в области информационной безопасности.

Также были следующие технические меры по обеспечению ИБ:

– выполнение сканирования ПЭВМ, используемых для ведения криминалистических учетов, на предмет неиспользуемых папок общего доступа и сетевых портов;

– обновление программного обеспечения антивирусной защиты на ПЭВМ пользователей центрального аппарата и территориальных подразделениях до актуальной версии, рекомендуемой производителем программного обеспечения;

– выполнение работ по замене серверов безопасности информационных систем (приобретение, установка);

– подключение ПЭВМ пользователей ведомственной СПД к серверу централизованного администрирования средствами антивирусной защиты;

– внедрение в ведомственную СПД DLP-системы, в перспективе – приобретение и внедрение SIEM системы;

– сканирование СПД организации на наличие уязвимостей в узлах вычислительной сети;

– составление и поддержание в актуальном состоянии карты сети передачи данных организации.

Предложенная методика проведения аудита информационной безопасности разрабатывалась в первую очередь для организаций, в информационных системах которых обрабатывается информация ограниченного распространения, не относящаяся к государственным секретам. Данная методика систематизирует подход к оценке информационной безопасности и позволяет выявить наиболее уязвимые элементы информационной системы организации. Также отчет, полученный в результате аудита, можно будет использовать для составления методологических указаний для сотрудников, ответственных за техническую защиту информации в областных Управлениях организации, что должно повысить уровень защищенности информационной системы путем расставления приоритетов при мониторинге ИС.

ЗАКЛЮЧЕНИЕ

На основе изученных в первой главе стандартов были использованы рекомендации, описанные в документах CIS Benchmark, о проверке соответствия требованиям ИБ конфигурации сети и настроек оборудования информационной системы организации для совершенствования методики внутреннего аудита ИБ. На основе международных стандартов ISO 27005, ISO/IEC 27001, и руководящих документов ФСТЭК России была разработана методика оценки актуальности угроз и уязвимостей информационной системы организации, результаты которой применены при количественной оценке рисков информационной безопасности. Рекомендации из библиотеки ITIL и специальных публикаций NIST были использованы при составлении рекомендуемых мер обеспечения ИБ (организационных и технических).

На основе анализа принятой методики проведения аудита организации были выявлены следующие недостатки: неполное покрытие возможных угроз ИБ, зацикленность аудита на внутренних нарушителях, отсутствие таких этапов, как вычисление уровня защищенности информационной системы и оценка уровня угроз ИБ.

Было принято решение совершенствовать методику путем внедрения в процесс проведения внутреннего аудита ИБ этапов идентификации актуальных угроз и уязвимостей ИС, и количественной оценки рисков ИБ.

На основе методики определения актуальных угроз безопасности информации, утвержденной ФСТЭК России, были определены уровни исходной защищенности информационной системы организации по трем показателям (территориальное размещение, наличие соединения с сетями общего пользования, разграничение прав пользователей). Далее на основе полученных значений была проведена оценка рисков реализации наиболее

вероятных для ИС организации угроз. Результат оценки показал, что актуальными угрозами для ИС организации являются следующие угрозы:

1 Воздействие вредоносного ПО – коэффициент реализуемости 0,65.

2 Утечка информации ограниченного распространения, в том числе нарушение инструкции по делопроизводству – 0,6.

3 Несанкционированное получение доступа к сети Интернет – 0,55.

4 Несанкционированное изменение конфигурации сетевого оборудования – 0,45.

Для активов организации была проведена количественная оценка рисков, учитывая изначальную ценность активов, вероятность реализации актуальных угроз и уязвимость активов перед угрозами. Финальное значение оценки риска может принимать значения от 1 до 150. К наиболее серьезным рискам были отнесены:

– реализация угроз «воздействие вредоносного ПО» и «несанкционированное получение доступа к сети Интернет» в отношении актива «ПЭВМ сотрудников» (значение риска 72);

– реализация угрозы «воздействие вредоносного ПО» в отношении активов «Сервера баз данных» и «Файловые сервера» (значение риска 80);

– реализация угрозы «утечка информации ограниченного распространения» в отношении активов «Сервера баз данных» и «Файловые сервера» (значение 105).

Для совершенствования методики было выбрано Управление Государственного комитета судебных экспертиз Республики Беларусь по Могилевской области, для него были определены и классифицированы информационные активы, выделены категории информации, обрабатываемой в информационной системе, описана система защиты информации, функционирующая в ИС подразделения.

Для учета процедуры оценки рисков ИБ для структурного подразделения было осуществлено совершенствование методики проведения внутреннего аудита. Методика была дополнена следующими этапами:

1 Идентификация угроз и уязвимостей. На этом этапе производится анализ угроз и уязвимостей информационной системы проверяемого подразделения с целью выявления актуальных угроз ИБ.

2 Оценка рисков. В этом этапе проводится оценка вероятности наступления угроз и их возможного воздействия на информационную систему подразделения и ее активы.

В процессе апробации была проведена количественная оценка рисков, характерных для Управления организации по Могилевской области. На основе результатов проведения аудита ИБ по усовершенствованной методике были описаны угрозы и уязвимости ИБ в выбранном подразделении, и были выявлены следующие нарушения политик ИБ:

– использование нелицензионного антивирусного программного обеспечения при наличии закупленных лицензионных продуктов;

– отсутствие настройки еженедельного сканирования компьютеров средствами антивирусной защиты;

– наличие несанкционированных подключений к сети Интернет;

– недостаточный контроль за распространением копий документов, содержащих информацию ограниченного распространения;

– неправильная конфигурация доступа к файлам компьютеров (наличие папок открытого доступа).

Для минимизации выявленных рисков и устранения последствий нарушения политик ИБ организации предложен ряд дополнительных мер обеспечения информационной безопасности, как организационных, так и технических.

Усовершенствованная методика применима в государственных организациях, в информационных системах которых обрабатывается информация, распространение которой ограничено, не отнесенная к государственным секретам, для минимизации рисков, затрагивающих наиболее критичные для деятельности организации активы. Также результаты аудита, полученные в процессе апробации, можно использовать как обоснование для дальнейшего совершенствования системы обеспечения информационной безопасности организации, при этом саму методику необходимо закрепить в качестве локального нормативно-правового акта подразделения, отвечающего за техническую защиту информации для дальнейшего применения на практике с целью обеспечения непрерывного процесса управления информационной безопасностью.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

Климович, А. Ю. Роль аудита информационной безопасности в обеспечении безопасности инфраструктуры информационных ресурсов/ Климович А.Ю. // Управление информационными ресурсами: материалы XVIII Международной научно-практической конференции, Минск, 10 марта 2022 г.; Академия управления при Президенте Республики Беларусь. / под ред. Е.С. Белоусовой – Минск, Академия управления при Президенте Республики Беларусь, 2022. – С. 251-252.