

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 3

Риски ИБ. Комплаенс

Спикер: Ануфриев Иван



ЗАНЯТИЕ 3.3

Подход к аудиту информационной безопасности



УСЛОВНОЕ РАЗДЕЛЕНИЕ ИНФОРМАЦИИ. «МЕТКИ» НА СЛАЙДАХ *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.	«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
		

Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»	Метки по используемым инструментам и практикам
		

Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
			



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ЗАНЯТИЯ

ВОПРОС 1: Compliance и методика

(COMPLIANCE)

Комплаенс при
проведении
аудита ИБ

(INSIGHTS)

Методика
проведения
аудита ИБ

(BEST PRACTICE)

Методика и
комплаенс на
практике



ВОПРОС 2: Результаты и рекомендации

(INSIGHTS)

Результаты аудита
ИБ.
Где должны быть
рекомендации

(BEST PRACTICE)

Рекомендации на
практике



ВОПРОС 3: Календарный план и расчет затрат

(INSIGHTS)

Календарный план
и расчет затрат

(BEST PRACTICE)

Календарный
план на практике



(BEST PRACTICE)

Расчет затрат на
практике:
калькуляция, БО



ВОПРОС 4: Системный подход

(BEST PRACTICE)

Привязка задач
аудита ИБ
к результатам

(BEST PRACTICE)

Пример аудита ИБ,
системный подход



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ЗАНЯТИЯ

ВОПРОС 1: Compliance и методика

(COMPLIANCE)

Комплаенс при
проведении
аудита ИБ

(INSIGHTS)

Методика
проведения
аудита ИБ

(BEST PRACTICE)

Методика и
комплаенс на
практике



ВОПРОС 2: Результаты и рекомендации

(INSIGHTS)

Результаты аудита
ИБ.
Где должны быть
рекомендации

(BEST PRACTICE)

Рекомендации на
практике



ВОПРОС 3: Календарный план и расчет затрат

(INSIGHTS)

Календарный план
и расчет затрат

(BEST PRACTICE)

Календарный
план на практике



(BEST PRACTICE)

Расчет затрат на
практике:
калькуляция, БО



ВОПРОС 4: Системный подход

(BEST PRACTICE)

Привязка задач
аудита ИБ
к результатам

(BEST PRACTICE)

Пример аудита ИБ,
системный подход





Основные требования, на соответствие которым проводится аудит ИБ

Основные Российские и международные НПА, стандарты



Общий аудит на соответствие законодательству РФ по ИБ

152-ФЗ, 149-ФЗ, 98-ФЗ,
документы ФСТЭК и ФСБ России и другие



Российские и международные стандарты

ISO/IEC 27001, ISO/IEC 27002, NIST 800, СТО БР, стандарты по процессам ИБ, ГОСТ Р ИСО 19011-2012, ГОСТ Р ИСО/МЭК 27007-2014 и другие.



Лучшие практики по обеспечению ИБ

Network Security Policy: Best Practices White Paper, Network Management System



Внутренние требования Заказчика

Выполнение особых задач, соответствие корпоративному комплаенсу



Заточенный аудит на соответствие нормативным требованиям, например по 187-ФЗ

Приказ ФСТЭК №235, №239. При проведении аудита опираемся на последовательность действий, которая выработана на основе ГОСТ Р ИСО 19011-2012 и методики ниже на следующем слайде



Отраслевые требования. Например Банк.

Отдельно для Банка аудит на соответствие требованиям Положения Банка России №382-П. Прилагаем опросник по НПС



Обследование	Категорирование информационных ресурсов	Анализ защищенности	Разработка рекомендаций
1. Сбор данных о процессах обработки защищаемой информации 2. Сбор данных об ИТ-инфраструктуре 3. Сбор данных о применяемых организационных и технических мерах защиты информации	1. Определение ресурсов, подлежащих защите 2. Определение владельцев ресурсов 3. Оценка степени критичности ресурсов 4. Формирование перечня ресурсов с указанием их критичности	1. Анализ применяемых технических мер защиты 2. Анализ процессов управления ИБ 3. Анализ организационно-распорядительных документов по ИБ 4. Анализ угроз ИБ 5. Анализ бизнес-процессов на наличие возможных каналов утечки информации 6. Инструментальный анализ защищенности	1. Методические указания и рекомендации по локализации, устранению и контролю выявленных недостатков 2. Рекомендации по внедрению дополнительных СЗИ 3. Рекомендации по разработке или доработке организационно-распорядительной документации 4. Рекомендации по устранению выявленных уязвимостей 5. Рекомендации по изменению конфигураций и настроек сетевых средств защиты информации.



МЕТОДИКА И КОМПЛАЕНС ПРИ ПРОВЕДЕНИИ АУДИТА ИБ НА ПРАКТИКЕ



(BEST PRACTICE)



Пример методики
Для корпоративной
сети



Методика аудита.pdf
(документ в приложении)

Содержание

1	АННОТАЦИЯ.....	3
2	ЦЕЛИ И ЗАДАЧИ ПРОВЕДЕНИЯ РАБОТ.....	4
3	МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПРОВЕДЕНИЯ РАБОТ.....	6
4	ОПИСАНИЕ СОСТАВА РАБОТ.....	10
4.1	СОГЛАСОВАНИЕ.....	11
4.2	СБОР И АНАЛИЗ.....	12
4.3	СБОР И АНАЛИЗ.....	13
4.4	ИДЕНТИФИКАЦИЯ.....	14
4.5	АНАЛИЗ ЗАЩИТЫ.....	15
4.6	РАЗРАБОТКА РЕКОМЕНДАЦИЙ.....	16

4 Описание состава работ

Описанный в настоящем разделе состав работ является предварительным и может быть уточнен при согласовании контрактных документов. Исполнитель выполняет только те работы, которые описаны в настоящем технико-коммерческом предложении.

Все работы по проведению обследования информационной безопасности предлагается проводить в соответствии с требованиями:

- согласование
- сбор и анализ
- сбор и анализ
- идентификация
- анализ защиты
- разработка

Прочие работы/документации, отчетов и могут быть выполнены

4.1 Согласование

На данном этапе ее части, подлежащей при проведении обслед. Границы обслед

3 Методологическая основа проведения работ

В качестве методологической основы, для проведения работ по обследованию информационной безопасности, рассматриваются следующие материалы:

- Стандарт ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования»;
- Стандарт ISO/IEC 27002 «Информационные технологии. Методы обеспечения безопасности. Свод практик по управлению информационной безопасностью»;
- Приказ ФСТЭК России №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;



2. РЕЗУЛЬТАТЫ И РЕКОМЕНДАЦИИ

ВОПРОС 1: Комплаенс и методика

COMPLIANCE

Комплаенс при
проведении
аудита ИБ

INSIGHTS

Методика
проведения
аудита ИБ

BEST PRACTICE

Методика и
комплаенс на
практике



ВОПРОС 2: Результаты и рекомендации

INSIGHTS

Результаты аудита
ИБ.
Где должны быть
рекомендации

BEST PRACTICE

Рекомендации на
практике



ВОПРОС 3: Календарный план и расчет затрат

INSIGHTS

Календарный план
и расчет затрат

BEST PRACTICE

Календарный
план на практике



BEST PRACTICE

Расчет затрат на
практике:
калькуляция, БО



ВОПРОС 4: Системный подход

BEST PRACTICE

Привязка задач
аудита ИБ
к результатам

BEST PRACTICE

Пример аудита ИБ,
системный подход





Какие должны быть результаты аудита ИБ

Учитывая требования бизнеса



Оценка состояния

Получена независимая оценка состояния ИБ



Идентификация активов

Идентифицированы информационные активы



Актуальные угрозы и РЕКОМЕНДАЦИИ

Выявлены актуальные угрозы ИБ
и предложены меры их нейтрализации



Актуальные уязвимости и РЕКОМЕНДАЦИИ

Выявлены уязвимости и предложены меры по их нейтрализации



Нормативный комплаенс и РЕКОМЕНДАЦИИ

Выявлены недостатки в обеспечении ИБ в соответствии с требованиями законодательства, стандартами, лучшими практиками и внутренними требованиями Заказчика и предложены меры по достижению соответствия



Корпоративный комплаенс и РЕКОМЕНДАЦИИ

Предложены меры по изменению организационно-распорядительной документации по ИБ и процессов управления ИБ



Сетевая безопасность и безопасность хостов и РЕКОМЕНДАЦИИ

Выявлены проблемы в организации сетевой безопасности и безопасности конечных устройств предложены меры по их устранению



План мероприятий

Подготовлен план мероприятий по достижению необходимого уровня ИБ (план мероприятий включает в себя бюджетную оценку их выполнения)



РЕКОМЕНДАЦИИ ПО РЕШЕНИЮ ВЫЯВЛЕННЫХ ПРОБЛЕМ НА ПРАКТИКЕ



(BEST PRACTICE)

(EXPERT TOOLS)

Примеры
подготовленных
рекомендаций
Для разных
типовых моделей
информационных
систем



Корреляция проблемы
рекомендации.xlsx
(документ в приложении)

№ п/п	Выявленные проблемы и недостатки	Рекомендации по повышению уровня ИБ	
3	Проблемы и недостатки во внутренних документах		
3.1	Не разработан план мероприятий по обеспечению защиты информации	1) Разработать план мероприятий по обеспечению защиты информации. План должен включать перечень будущих мероприятий в области ИБ (внедрение СЗИ, разработка или актуализация ОРД, обучение работников, модернизация функционала ИС в части безопасности и др.), сроки исполнения мероприятий, ответственных лиц и исполнителей.	
3.2	Действующий (разработанный) не соответствует	№ п/п	Выявленные проблемы и недостатки
2	Проблемы и недостатки в обеспечении ИБ, не связанные с сетевой безопасностью		
2.1	Низкий уровень защищенности серверов ОИК и видеоконтроллеров ИС «СК»: - используются устаревшие версии ОС (на видеоконтроллерах установлена ОС MS Windows XP); - используется устаревшая версия RAdmin; - не форсирован строгий контроль; - отсутствует видеоконтроль	1) При наличии технической возможности установить на видеоконтроллеры ИС «СК» ОС MS Windows версии не ниже MS Windows 7 (со всеми актуальными обновлениями). 2) Разрешить на уровне МЭ взаимодействие SMART-FEP, серверов ОИК и видеоконтроллеров только с ограниченным кругом хостов в ЛВС Заказчика. 3) На уровне ОС и Radmin разрешить подключение к серверам ОИК и видеоконтроллерам только ограниченному кругу пользователей. Перечень пользователей, допущенных до подключения зафиксировать документально. 4) Исключить возможность подключения к серверам ОИК «СК-2007» и видеоконтроллерам внешних носителей	
3.3	Не предоставлены внешние управляющие пользователи	№ п/п	Выявленные проблемы и недостатки
1	Проблемы и недостатками в обеспечении ИБ на уровне сети		
1.1	В ИС SAP не реализована отказоустойчивость следующего сетевого оборудования: - маршрутизаторы Cisco 3945, Cisco 3925, Voice, Outside; - межсетевые экраны Cisco ASA Internet, Cisco ASA vrb.	1) Внедрить резервные маршрутизаторы Cisco 3945, Cisco 3925, Cisco 2921 (или аналогичные) в дополнение к каждому из устройств Cisco 3945, Cisco 3925, Voice, соответственно. Для маршрутизаторов полная идентичность не обязательна, достаточно установить модель с таким же набором интерфейсов и с такой же производительностью. Для обеспечения отказоустойчивости маршрутизаторов необходимо настроить протокол резервирования шлюза, например HSRP. 2) Внедрить МЭ Cisco ASA 5555-X (2 шт.) вместо МЭ Cisco ASA Internet. Настроить режим отказоустойчивости на внедренных МЭ. 3) Установить с избыточностью коммутаторы, через которые подключены маршрутизаторы Cisco 3945, Cisco 3925, Voice, Outside и межсетевые экраны Cisco ASA Internet, Cisco ASA vrb.	
1.2	Передача защищаемой информации в открытом виде при передаче данных по каналам связи, выходящим за пределы ИЗ (каналы связи ЦОД с филиалами и производственными отделениями) при взаимодействии систем ЦОД Заказчика с системами сторонних организаций	1) Настроить на маршрутизаторах Cisco 3925 и Cisco 3945 в ЦОД и на соответствующих маршрутизаторах филиалов и их производственных отделений IPSec Site to Site VPN для связи со всеми филиалами Заказчика и производственными отделениями филиалов (в случаях, когда по каналам связи передается защищаемая информация). 2) Сконфигурировать в качестве алгоритма шифрования AES-128 или AES-256. Ключ аутентификации должен удовлетворять требованиям сложности: состоять из буквенно-цифровых символов с учетом заглавных и прописных букв в латинском алфавите, знаков препинания и специальных символов, длина ключа должна составлять не менее 32 символов, а сам он не должен нести смысловой нагрузки.	
1.3	- Применяется локальная схема аутентификации без использования централизованного сервера для управления маршрутизаторами, коммутаторами и межсетевыми экранами; - не используется парольная политика для управления сетевым оборудованием; - используется одна учетная запись для управления сетевым оборудованием.	1) Внедрить сервер централизованной аутентификации Cisco ISE 2.0, работающий по протоколу TACACS. Обеспечить подключение администраторов маршрутизаторов, коммутаторов и межсетевых экранов к данным сетевым устройствам по личным именам пользователей и паролям. На самих сетевых устройствах завести только одну учетную запись, которая будет использоваться только в крайних случаях – при отсутствии связи с TACACS сервером. 2) Внедрить дополнительный сервер Cisco ISE 2.0 для обеспечения отказоустойчивости. 3) Настроить на серверах Cisco ISE 2.0 парольную политику, в соответствии с требованиями подраздела 6.7 Положения по ЗИ: - длина пароля не менее 8 символов; - в составе пароля должны быть латинские буквы в верхнем и нижнем регистре, цифры и специальные символы; - в пароле должна отсутствовать смысловая нагрузка; - частота смены пароля – 1 раз в 2 месяца.	
	Не применяется двухфакторная		



3. КАЛЕНДАРНЫЙ ПЛАН И РАСЧЕТ ЗАТРАТ

ВОПРОС 1: Комплаенс и методика

(COMPLIANCE)

Комплаенс при
проведении
аудита ИБ

(INSIGHTS)

Методика
проведения
аудита ИБ

(BEST PRACTICE)

Методика и
комплаенс на
практике



ВОПРОС 2: Результаты и рекомендации

(INSIGHTS)

Результаты аудита
ИБ.
Где должны быть
рекомендации

(BEST PRACTICE)

Рекомендации на
практике



ВОПРОС 3: Календарный план и расчет затрат

(INSIGHTS)

Календарный план
и расчет затрат

(BEST PRACTICE)

Календарный
план на практике



(BEST PRACTICE)

Расчет затрат на
практике:
калькуляция, БО



ВОПРОС 4: Системный подход

(BEST PRACTICE)

Привязка задач
аудита ИБ
к результатам

(BEST PRACTICE)

Пример аудита ИБ,
системный подход



Что необходимо учитывать

При составлении календарного плана и бюджета аудита ИБ



Рамки проведения аудита

Необходимо в равной степени учитывать организационный, технологический, и программно-технический уровни обеспечения информационной безопасности ИБ



Области детального изучения

основное внимание должно уделяться компонентам и подсистемам, осуществляющим обработку конфиденциальной информации компании



Требуемый уровень детализации и полноты

Для получения адекватных результатов необходимо провести базовый анализ, для полноты – требуется провести детальный анализ, цель которого - количественно оценить уровень информационной безопасности компании на основе специальных количественных метрик и мер ИБ



Формализация оценок уровня безопасности компании

Определяются качественные и количественные параметры для получения объективных оценок уровня информационной безопасности компании



Требования ИБ

Фиксируется обоснованный выбор требований информационной безопасности, определяются критерии и показатели оценки информационной безопасности компании, выбираются количественные метрики и меры безопасности



Исходные данные для проведения аудита

Помимо стандартных исходных данных могут использоваться и дополнительные исходные данные, специфичные для каждой конкретной компании, например статистика нарушений политики безопасности компании, статистика внешних и внутренних атак, уязвимости наиболее критичных корпоративных информационных ресурсов



Пример календарного
плана работ аудита ИБ

С учетом используемых стандартов
и векторов проведения аудита ИБ

Календарный план работ

Общий план работ представлен в таблице 1. Выполнение некоторых этапов работ может проводиться Исполнителем параллельно.

Таблица 1. План работ

№ п/п	Этап	Описание	Закрывающие документы	Длительность, мес.
1.	Согласование границ проведения обследования	Определение рамок и границ объекта обследования	Акт о границах проведения обследования информационной безопасности	0.25
2.	Сбор и анализ исходных данных об информационной системе	Сбор и анализ данных о сетевом и серверном оборудовании информационной инфраструктуры и корпоративной информационной системы, сбор и анализ данных об информационных потоках	Структурированная информация о корпоративной информационной системе Заказчика	0.5
3.	Сбор исходных данных о состоянии защищенности информационных ресурсов	1 Анализ используемых средств и методов защиты информации, их размещения, настройки, режимов взаимодействия и эксплуатации; 2 инструментальный анализ защищенности; 3 оценка полноты и эффективности применяемых мер защиты и информации, включая оценку полноты организационно-распорядительной документации; 4 анализ организационно-распорядительной документации; 5 Анализ угроз ИБ.	- Модель угроз информационной безопасности; - Перечень объектов Заказчика, в отношении которых возможна реализация угроз несанкционированного доступа.	1
4.	Идентификация информационных активов	1 Формирование отчетных документов по результатам выполнения всех работ; 2 подготовка рекомендаций по устранению выявленных недостатков.	- Описание корпоративной информационной системы Заказчика; - Отчет по результатам анализа эффективности применяемых мер защиты информации; - Отчет о выявленных уязвимостях и рекомендации по их устранению; - Рекомендации по совершенствованию или построению системы информационной безопасности (включая предложения по разработке/доработке организационно-распорядительной документации); - Детальный календарный план мероприятий необходимых для устранения выявленных недостатков и повышения степени защищенности корпоративных информационных ресурсов.	1.5
ИТОГО:				4



Календарный план.pdf
(документ в приложении)





Архитектор		Итого, часов	Итого, руб	
	ставка / стоимость			Коэффициент к базовой ставке
	3 650,00 Р			1
	438 000,00 Р	160	533 392,40 Р	
	438 000,00 Р	160	533 392,40 Р	
	0,00 Р	20	47 696,20 Р	
	0,00 Р	80	190 784,80 Р	
	292 000,00 Р	160	482 784,80 Р	
	0,00 Р	120	286 177,20 Р	
30	292 000,00 Р	400	1 055 139,20 Р	
60	584 000,00 Р	240	774 784,80 Р	



4. СИСТЕМНЫЙ ПОДХОД К АУДИТУ ИБ

ВОПРОС 1: Комплаенс и методика

(COMPLIANCE)

Комплаенс при
проведении
аудита ИБ

(INSIGHTS)

Методика
проведения
аудита ИБ

(BEST PRACTICE)

Методика и
комплаенс на
практике



ВОПРОС 2: Результаты и рекомендации

(INSIGHTS)

Результаты аудита
ИБ.
Где должны быть
рекомендации

(BEST PRACTICE)

Рекомендации на
практике



ВОПРОС 3: Календарный план и расчет затрат

(INSIGHTS)

Календарный план
и расчет затрат

(BEST PRACTICE)

Календарный
план на практике



(BEST PRACTICE)

Расчет затрат на
практике:
калькуляция, БО



ВОПРОС 4: Системный подход

(BEST PRACTICE)

Привязка задач
аудита ИБ
к результатам

(BEST PRACTICE)

Пример аудита ИБ,
системный подход



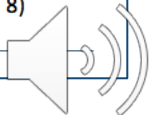


Пример таблицы привязки задач аудита ИБ к результатам. И ссылки на разделы.



Задача_результат.pdf
(документ в приложении)

№ п/п	Задача аудита ИБ	Полученный результат	Ссылка на раздел Отчета
1	Анализ соответствия применяемых мер защиты информации на уровне сети требованиям российского законодательства и внутренних документов Заказчика		
1.1	Анализ действующих нормативных и распорядительных Заказчика по ИБ	Проведена оценка соответствия действующих нормативных и организационно-распорядительных актов политик межсетевых экранов на возможность НСД из сети Интернет	Настоящий отчет
1.2	Анализ применяемых организационных и мер защиты информа	Определение критичных для ИС и ЛВС Заказчика УБИ (с указанием объектов воздействия угроз и нарушаемых характеристик	Настоящий отчет (подраздел 5.3)
3	Определение критичных угроз безопасности информации		
5	Разработка плана мероприятий по повышению уровня ИБ		
5.1	Разработка плана мероприятий по повышению уровня информационной безопасности в Заказчике позволяющего устранить выявленные в процессе аудита информационной безопасности проблемы и недостатки	Разработан план мероприятий по повышению уровня ИБ Заказчика, содержащий предлагаемые Исполнителем к выполнению организационные и технические мероприятия, позволяющие устранить выявленные в процессе аудита проблемы и недостатки	Настоящий отчет (раздел 7)
	Заказчиком подготовленных Исполнителем рекомендаций	корпоративной сети и по устранению выявленных в процессе аудита ИБ проблем и недостатков	Настоящий отчет (раздел 8)
	Разработка рекомендаций по повышению уровня ИБ		
	ахий по хнической ной сети	Подготовлены рекомендации по изменению технической архитектуры корпоративной сети в целях повышения уровня информационной безопасности, а также соответствия принципам построения защищенных сетей	Настоящий отчет (подраздел 6.1)
	ахий по нных в роблем и	Разработаны подробные рекомендации по устранению выявленных в процессе аудита ИБ проблем и недостатков	Настоящий отчет (подраздел 6.2)
	пективной мы сети, исполнение	Разработана перспективная L3 схема сети, учитывающая выполнение Заказчиком рекомендаций по изменению технической архитектуры	Настоящий отчет (раздел 8)



СИСТЕМНЫЙ ПОДХОД К АУДИТУ ИБ

(BEST PRACTICE)

(EXPERT
TOOLS)



СОДЕРЖАНИЕ

Пример аудита ИБ

Для технологического
и корпоративного
сегментов

УТВЕРЖДАЮ
ООО «ЗАКАЗЧИК»

Функциональный заказчик
(директор по ИБ)

_____ ФИО
«__» _____ 2022 г.

УТВЕРЖДАЮ
ООО «ИСПОЛНИТЕЛЬ»

Генеральный директор

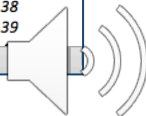
_____ ФИО
«__» _____ 2022 г.

Отчет об аудите информационной безопасности корпоративной сети ООО «Заказчик»

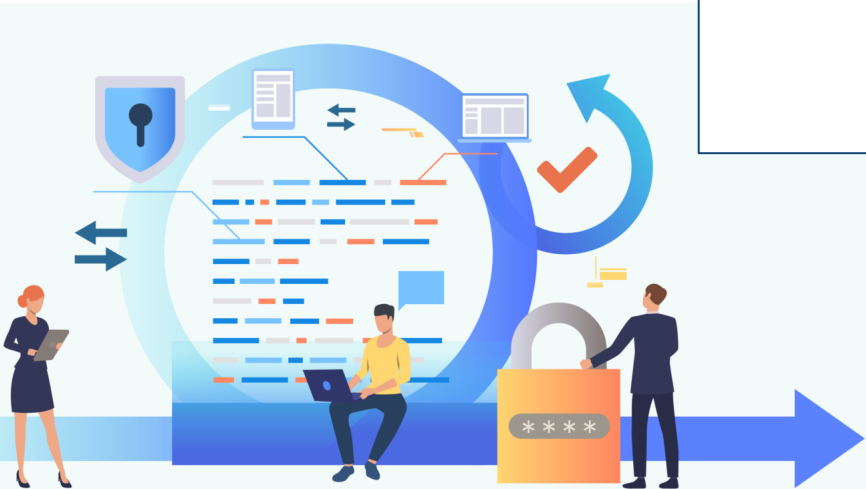


Содержание

1	ТЕРМИНЫ И СОКРАЩЕНИЯ.....	6
2	ЦЕЛИ И ЗАДАЧИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	11
3	КРАТКАЯ СВОДКА ПО ОТЧЕТУ.....	13
4	ОПИСАНИЕ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	16
4.1	ИНФОРМАЦИОННАЯ СИСТЕМА «ИС-1»	16
4.1.1	Назначение системы и обрабатываемые данные	16
4.1.2	Пользователи информационной системы	17
4.1.3	Смежные системы.....	18
4.1.4	Архитектура системы	19
4.2	АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ РЕМОНТАМИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ	21
4.2.1	Назначение системы и обрабатываемые данные	21
4.2.2	Пользователи информационной системы	21
4.2.3	Смежные системы.....	22
4.2.4	Архитектура системы	22
4.3	ПРОГРАММНЫЙ КОМПЛЕКС «АВАРИЙНОСТЬ»	23
4.3.1	Назначение системы и обрабатываемые данные	23
4.3.2	Пользователи информационной системы	24
4.3.3	Смежные системы.....	26
4.3.4	Архитектура системы	26
4.4	СИСТЕМА УПРАВЛЕНИЯ УСЛУГАМИ ПО ТРАНСПОРТИРОВКЕ ЭЛЕКТРОЭНЕРГИИ И СИСТЕМА УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ АКТИВАМИ	27
4.4.1	Назначение систем и обрабатываемые данные	27
4.4.2	Пользователи информационных систем	27
4.4.3	Смежные системы.....	28
4.4.4	Архитектура систем	28
4.5	КОРПОРАТИВНЫЙ ПРОГРАММНЫЙ КОМПЛЕКС «ТЕХНОЛОГИЧЕСКОЕ ПРИСОЕДИНЕНИЕ»	30
4.5.1	Назначение системы и обрабатываемые данные	30
4.5.2	Пользователи информационной системы	30
4.5.3	Смежные системы.....	32
4.5.4	Архитектура системы	32
4.6	ЕДИНАЯ КОРПОРАТИВНАЯ УЧЕТНАЯ СИСТЕМА ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ	33
4.6.1	Назначение системы и обрабатываемые данные	33
4.6.2	Пользователи информационной системы	35
4.6.3	Смежные системы.....	36
4.6.4	Архитектура системы	37
4.7	СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	38
4.7.1	Назначение системы и обрабатываемые данные	38
4.7.2	Пользователи информационной системы	39



Структура аудита ИБ и
отчет по аудиту ИБ
корпоративной сети
предприятия.pdf
(документ в приложении)



**Благодарю
за внимание!**

