


Стандарт предприятия

Аудит информационной безопасности

Введен впервые

УТВЕРЖДАЮ
Генеральный директор
ООО «Эн+ Диджитал»

 А. А. Герасименко
10.10.2018

(дата)

Введен в действие приказом
ООО «Эн+ Диджитал»
от 08.10.18г. № 23

ООО «Эн+ Диджитал»

Содержание

Содержание	2
Введение	3
1. Область применения.....	3
2. Сокращения и определения	3
3. Общие сведения	3
4. Виды аудитов	4
5. Проведение аудита ИБ	5
6. Результаты проведения аудита.....	6
7. Ответственность.....	6
Приложение 1	7
Методология проведения аудита ИБ.....	7
Лист регистрации изменений	25

Введение

Настоящий стандарт предприятия разработан в целях описания процесса осуществления внутренних и независимых аудитов информационной безопасности ООО «Эн+ Диджитал» (далее – Компания).

1. Область применения

1.1. Настоящий стандарт устанавливает в Компании:

1.1.1 нормативную базу для деятельности аудиторов ИБ;

1.1.2 полномочия аудиторов ИБ;

1.1.3 ответственность аудиторов за обеспечение ИБ и штатного (нормального) режима функционирования информационных систем Компании, подвергающихся аудиторским проверкам ИБ;

1.1.4 порядок и условия проведения аудита ИБ.

1.2. Настоящий стандарт предприятия распространяется на все подразделения Компании прямо или косвенно задействованные в проведении аудита ИБ.

1.3. Настоящий стандарт предприятия распространяется на лиц, не являющихся работниками Компании, проводящих аудит ИБ автоматизированных и телекоммуникационных систем Компании, при наличии заключенных договоров, в которых устанавливаются их права и обязанности в области информационной безопасности со ссылками на стандарты предприятия.

1.4. Настоящий стандарт предприятия входит в состав нормативных документов системы управления Компании.

2. Сокращения и определения

2.1. В настоящем стандарте используются следующие сокращения и определения:

ИБ – информационная безопасность;

ИТ-инфраструктура – инфраструктура информационных технологий.

2.2. В настоящей политике используются следующие определения:

Аудитор ИБ – эксперт или группа экспертов по информационной безопасности, в обязанности которых входит проведение аудита ИБ и формирование рекомендаций по устранению рисков ИБ, выявленных в ходе аудита ИБ;

ИТ служба – подразделение (работник) Общества, осуществляющее функции ИТ обеспечения Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг;

ИТ-инфраструктура – организационно-техническое объединение информационных систем, связей между ними и эксплуатационного персонала, обеспечивающее предоставление информационных, вычислительных и телекоммуникационных ресурсов, возможностей и услуг;

Компания – ООО «Эн+ Диджитал», а также партнеры, являющиеся пользователями или администраторами информационных систем ООО «Эн+ Диджитал», подписавшие соответствующие соглашения;

Подразделения ИБ – подразделение (работник), ответственное за контроль обеспечения ИБ Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

3. Общие сведения

3.1. Аудит информационной безопасности является одним из основных средств контроля управленческих, операционных и технических мер защиты информации, реализуе-

мых в Компании.

3.2. Область проведения аудита ИБ охватывает все информационные активы, информационные системы, технические средства, программные средства и прочие активы (которые связаны с информационными), принадлежащие Компании.

3.3. Аудит ИБ проводится в целях:

3.3.1 получения объективных данных о текущем состоянии обеспечения ИБ Компании, в том числе эффективности применяемых организационных и технических мер защиты от внешних и внутренних угроз ИБ;

3.3.2 оценки рисков, связанных с осуществлением угроз ИБ в отношении информационных активов Компании;

3.3.3 оценки достаточности реализованных в Компании мер по защите информации и их соответствия политике и стандартам информационной безопасности Компании;

3.3.4 разработка краткосрочных (оперативных рекомендаций) по повышению уровня защищенности, разработка долгосрочных планов развития системы обеспечения информационной безопасности;

3.3.5 выявления уязвимостей ИТ-инфраструктуры и принятия мер по их устранению.

3.4. Для достижения указанных целей в процессе проведения аудита ИБ решаются следующие задачи:

3.4.1 сбор и анализ исходных данных о ключевых бизнес-процессах, информационных активах, организационном и функциональном устройстве ИТ-инфраструктуры Компании;

3.4.2 оценка архитектуры и конфигурации компонентов ИТ-инфраструктуры и существующих технических средств и мер защиты информации;

3.4.3 анализ существующих локальных нормативных документов по ИБ (политик, стандартов, регламентов, инструкций и т.д.) на предмет полноты и эффективности устанавливаемых требований к обеспечению ИБ, а также анализ проектной и эксплуатационной документации на системы и средства защиты и ключевые информационные системы;

3.4.4 оценка существующей реализации процессов управления ИБ;

3.4.5 проведение инструментального анализа состояния защищенности ИТ-инфраструктуры, эффективности средств и мер защиты информации;

3.4.6 формирование рекомендаций по разработке (или доработке) локальных нормативных документов по ИБ или создание типовых документов;

3.4.7 формирование предложений по использованию существующих и установке дополнительных средств защиты информации для повышения уровня надежности и безопасности ИТ-инфраструктуры Компании.

3.5. Исходя из указанных целей в рамках настоящего стандарта аудит состояния ИБ подразделяется на три стадии:

3.5.1 проведение аудиторских проверок, определение рисков ИБ и их влияния на риски бизнес-процессов Компании;

3.5.2 разработка краткосрочных рекомендаций по повышению уровня защищенности и составление итогового отчета;

3.5.3 разработка программы действий по устранению выявленных недостатков и реализация корректирующих мер.

4. Виды аудитов

4.1. Внешний аудит проводится внешними аудиторами ИБ на основании заключенных договоров, по мере необходимости. Внешние аудиторы ИБ могут использовать свою методологию аудита или методологию Компании, указанную для внутреннего аудита (Приложе-

ние 1). Он производится независимыми экспертами из аудиторских фирм и организаций, специализирующихся на вопросах защиты информации и имущих соответствующую лицензию.

4.2. Внутренний аудит ИБ разделяется на аудит плановый и оперативный контроль.

4.3. Плановый аудит проводится на регулярной основе в соответствии с расписанием проведения аудитов информационной безопасности.

4.4. Оперативный контроль состояния ИБ проводится по мере необходимости. Он применяется для выявления недостатков в тех областях, где плановый аудит не позволит своевременно их определить. Основаниями для него может послужить следующее:

4.4.1 истечение срока исполнения программы действий по устранению выявленных недостатков (нарушений, наблюдений);

4.4.2 поступление руководству Компании, работникам подразделения ИБ сообщений об авариях, инцидентах или обращениях от работников о фактах нарушения ИБ;

4.4.3 распоряжения руководителей (директора по направлениям деятельности, заместители генерального директора, генеральный директор) Компании для выявления фактов нарушения ИБ;

4.4.4 нарушение прав и законных интересов работников Компании.

5. Проведение аудита ИБ

5.1. Аудиторам ИБ предоставляются необходимые права доступа к информационным активам Компании, а также все сведения необходимые для проведения проверок, включая:

5.1.1 физический и логический доступ к программным и техническим средствам, являющимся собственностью Компании с полномочиями, достаточными для проведения проверок;

5.1.2 доступ к сведениям и документам, необходимым для проведения аудиторских проверок;

5.1.3 доступ в проверяемые помещения;

5.1.4 возможность мониторинга сетевого трафика и анализа информационных потоков как внутренних, так и с внешними сетями;

5.1.5 возможность регистрации и анализа системных событий на технических и программных средствах Компании (серверах, рабочих станциях и активном сетевом оборудовании корпоративной сети).

5.2. Проведение внешнего аудита ИБ:

5.2.1 Физический и логический доступ к информационным системам Компании предоставляется внешним аудиторам ИБ только по согласованию подразделения ИБ. Внешние аудиторы ИБ могут проводить работы только под контролем работников подразделения ИБ или работников ИТ службы. Внешние аудиторы ИБ в обязательном порядке заключают договор о неразглашении конфиденциальной информации.

5.2.2 Руководители подразделений, участвующие во внешнем аудите уведомляют не менее чем за 48 часов до проверки, инициатором аудита. Предоставление информации внешним аудиторам ИБ разрешается только по согласованию с владельцами информации.

5.3. Внутренний аудит ИБ может производить непосредственно как работники подразделения ИБ, так и работники подразделений Компании, обеспечивающие защиту информационных активов.

5.4. Работники подразделений Компании обязаны оказывать аудитору ИБ содействие в проведении проверок и оперативно предоставлять необходимые сведения по запросам аудитора ИБ.

5.5. Плановый аудит ИБ производится следующим образом:

- 5.5.1 подготавливается расписание аудитов ИБ на год;
- 5.5.2 применяется методология проведения аудита ИБ (Приложение 1);

5.6. Проведение оперативного контроля состояния ИБ:

5.6.1 аудитор ИБ определяет объем и шаги контроля как в плановом аудите, однако он вправе изменять объем и шаги контроля в зависимости от критичности ситуации, временных ограничений и других важных факторов;

5.6.2 если нарушение ИБ причиняет или может причинить значительный вред Компании или её работникам, а также существует высокая вероятность реализации такой угрозы, то об этом немедленно ставится в известность руководитель подразделения ИБ;

5.6.3 могут использоваться технические средства сбора информации и/или тестирования уязвимостей;

5.6.4 проведение оперативного контроля согласовывается руководителем подразделения ИБ.

6. Результаты проведения аудита

6.1. Результатом проведения:

6.1.1 внешнего аудита ИБ является аудиторский отчет, который готовится в соответствии с выбранной методологией аудита, и направляется инициатору проведения аудита;

6.1.2 планового аудита ИБ является аудиторский отчет с реестром недостатков, направляемый аудитором ИБ, на имя руководителя проверяемого структурного подразделения Компании;

6.1.3 оперативного контроля состояния ИБ является аудиторский отчет в виде справки или иного документа, который предоставляется инициатору проведения проверки, и может являться официальным документом при проведении служебных расследований.

6.2. На основании аудиторского отчета руководителями структурных подразделений, ответственными за планирование мер защиты, совместно с аудитором ИБ в месячный срок разрабатывается программа действий по устранению выявленных недостатков (нарушений, наблюдений) системы защиты информации. В рамках реализации программы действий назначаются исполнители по реализации мер защиты и сроки выполнения этих работ. Контроль подготовки и выполнения программы по реализации контрмер возлагается на Менеджера ИБ.

6.3. На основании разработанного плана действий исполнители в согласованный с подразделением ИБ срок, производят устранение выявленных недостатков.

7. Ответственность

7.1. Ответственность за организацию и проведение внутреннего аудита ИБ в соответствии с требованиями настоящего стандарта, утвержденными методологиями и планами проведения аудита возлагается на Менеджера ИБ.

7.2. На аудитора ИБ возлагается ответственность за выполнение действий с использованием предоставленных для проведения аудитов и оперативных контролей ИБ прав.

7.3. Руководители структурных подразделений Компании несут ответственность за выполнение положений настоящего стандарта в подконтрольных им подразделениях в части предоставления аудитору ИБ информации, необходимой для проведения аудита и реализации программы контрмер.

Методология проведения аудита ИБ

1. Последовательность этапов проведения работ

Графическое отображение порядка проведения аудита представлено схематично на Рисунке 1.



Рис. 1. Порядок проведения аудита состояния информационной безопасности.

1.1. Обязательные этапы первой стадии:

- Сбор исходных данных об объекте аудита;
- Анализ локальных нормативных документов по ИБ, утвержденных в Компании;
- Оценка ИТ-инфраструктуры и применяемых средств и мер ИБ;
- Оценка существующей реализации процессов управления ИБ;
- Проведение инструментальных проверок;
- Анализ выявленных уязвимостей и недостатков и связанных с ними угроз.

1.2. Необязательные этапы первой стадии:

- Анализ физической безопасности;
- Проведение тестов на проникновение с использованием методов социальной инженерии.

1.3. Обязательные этапы второй стадии:

- Выработка краткосрочных рекомендаций по устранению выявленных недостатков системы обеспечения ИБ;
- Составление итогового отчета.

1.4. Обязательные этапы третьей стадии:

- Программа действий по устранению выявленных недостатков и реализации корректирующих мер.

1.5. Необязательные этапы третьей стадии:

- Разработка плана развития ИБ и оценка стоимости проектов.

2. Сбор исходных данных

Сбор исходных данных происходит в процессе организационного аудита и инструментального аудита.

3. Анализ локальных нормативных документов по ИБ

В рамках данного этапа осуществляется анализ документации по ИБ, утверждённой в Компании, с целью выявления недостатков.

Недостатками в системе локальной нормативной документации считаются:

- в целом отсутствие документа(ов), определяющих порядок и требования к конкретным процессам ИБ, а также организационным и техническим мерам обеспечения ИБ;
- неполнота, отсутствие объективности и адекватности требований ИБ, установленных локальными нормативными документами, а также несоответствие требований существующим рисками ИБ;
- противоречие или несоответствие требованиям законодательства и ведомственным нормативным документам.

В рамках проводимого аудита оценке подлежат следующие категории локальных нормативных документов:

- Политика информационной безопасности Компании, устанавливающая позицию руководства Компании к обеспечению ИБ, общие подходы и требования, и являющаяся ключевым документом для всей структуры локальных нормативных актов по ИБ Компании;
- Частные политики, положения и корпоративные стандарты, определяющие правила, принципы и требования по конкретным процессам и мерам ИБ.
- Регламенты и инструкции, определяющие требования к процедурам обеспечения ИБ, выполняемым сотрудниками (специалистами по ИТ и ИБ) и реализующих требования частных политик и положений.

Критерии для оценки системы локальных нормативных актов по ИБ приведены в Таблице 1. В процессе аудита перечень может быть изменен и/или дополнен.

Таблица 1

Критерии для оценки системы локальных нормативных актов

№	Название документа	Результат	Недостатки в документации	Рекомендации по устранению недостатков
Документы 1-го уровня				
1.	Политика информационной безопасности			
Документы 2-го уровня				
2.	Стандарт антивирусной защиты			
3.	Стандарт аудит ИБ			
4.	Стандарт установки обновлений ПО			

№	Название документа	Результат	Недостатки в документации	Рекомендации по устранению недостатков
5.	Стандарт по паролям (идентификации и аутентификации)			
6.	Стандарт управления доступом			
7.	Стандарт межсетевого взаимодействия			
8.	Стандарт резервного копирования			
9.	Стандарт управления инцидентами ИБ			
10.	Стандарт защита КИ			
Документы 3-го уровня				
11.	Инструкция по антивирусной защите			
12.	Методика проведения аудита ИБ			
13.	Регламент установки обновления ПО			
14.	Регламент предоставления доступа			
15.	Регламент резервного копирования			
Организационно-распорядительные документы				
16.	Приказ «О служебной переписке»			
17.	Приказ «О реализации программы повышения осведомленности сотрудников по вопросам ИБ»			

4. Оценка ИТ-инфраструктуры и применяемых средств и мер ИБ

Целью данного этапа является главным образом сбор и анализ информации об архитектуре и конфигурации элементов ИТ-инфраструктуры, существующих технических средствах и мерах защиты информации. Результатом анализа полученной информации должно стать максимально полное выявление существующих недостатков в ИТ-инфраструктуре, средствах и мерах обеспечения ИБ.

Необходимо стремиться к тому, что все недостатки системы обеспечения ИБ должны быть обнаружены до начала следующего этапа аудита – инструментального анализа, а сами инструментальные проверки должны только подтвердить предположения и являться наглядным свидетельством существующих недостатков системы обеспечения ИБ и как следствие угроз ИБ.

Работы, проводимые в рамках данного этапа, включают:

- Анализ проектной и эксплуатационной документации на информационные системы и средства (системы) защиты информации;
- Аудит конфигураций безопасности сетевой инфраструктуры;
- Аудит конфигураций безопасности операционных систем;
- Аудит конфигураций безопасности информационных системы

- Аудит конфигурации безопасности системы виртуализации;
- Аудит конфигураций безопасности мобильных устройств;
- Аудит конфигураций систем и средств защиты информации.

Отдельно необходимо провести анализ конфигураций безопасности автоматизированных рабочих мест, с которых осуществляется взаимодействие с системами дистанционного банковского обслуживания (далее – АРМ ДБО), как систем, угрозы ИБ которых несут прямые финансовые риски:

- Аудит правил межсетевого взаимодействия АРМ ДБО с сегментами корпоративной сети и сетью Интернет;
- Аудит конфигураций безопасности операционных систем;
- Аудит конфигураций безопасности программного обеспечения систем АРМ ДБО.

При проведении аудита конкретной Компании перечень работ может быть расширен на усмотрение руководителя подразделения ИБ исходя из конкретных особенностей ИТ-инфраструктуры Компании.

Сбор информации в рамках данного этапа может состоять из:

- Интервьюирование сотрудников Компании, ответственных за ИТ и ИБ и ключевые бизнес-процессы;
- Изучения проектной и эксплуатационной документации на информационные системы и системы защиты информации, предоставленной в рамках проведения аудита сотрудниками Компании;
- Изучения конфигураций элементов ИТ-инфраструктуры;
- Проверка заявленной функциональности и реализованных мер (к примеру, если утверждается, что для учетных записей с правами администраторов домена запрещен вход на рабочие станции, то проверка заключается в попытке аутентификации под данной учетной записью на рабочей станции).

Критерии для оценки сетевой инфраструктуры, применяемых средств и мер ИБ приведены в Таблице 2. В процессе аудита перечень может быть изменен и/или дополнен.

Таблица 2

Критерии для оценки сетевой инфраструктуры, применяемых средств и мер ИБ

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
Безопасность взаимодействия КСПД с сетью Интернет						
1.	Ресурсы КСПД, доступные из сети Интернет, выведены в ДМЗ и отделены от внутренних сегментов и сети Интернет посредством МЭ					
2.	На периметре КСПД установлен МЭ класса NGFW, предусмотрено кластерное резервирование					

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
3.	На периметре КСПД осуществляется контроль трафика приложений и контроль доступа к Web-ресурсам					
4.	На периметре КСПД осуществляется инспекция HTTPS трафика, антивирусная проверка, обнаружение соединений с C&C					
5.	На границе КСПД с сетью Интернет применяется IPS. Базы сигнатур регулярно обновляются. События IPS анализируются					
Контроль межсетевых взаимодействий						
6.	Схема сети документирована, находится в актуальном состоянии.					
7.	В КСПД выделены минимально необходимые сегменты: серверный, пользовательский, сегмент систем ИБ, сегмент коммутационного оборудования.					
8.	Межсетевые взаимодействия ограничены только необходимыми и документированными разрешающими правилами фильтрации трафика					
9.	Для гостевых беспроводных сетей ограничено взаимодействие между клиентами сети и остальными сегментами КСПД					
10.	Изменение правил межсетевого экранирования осуществляется на основании заявок, согласованных специалистов по ИБ					
11.	Проводится регулярный аудит на предмет избыточности разрешающих правил МЭ					
12.	Задействован механизм защиты от подмены IP-адресов (Anti-Spoofing)					
13.	Регистрация событий системы межсетевого экранирования					
Безопасность управления сетью						

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
14.	Ограничен сетевой доступ к управляющим интерфейсам сетевого оборудования: интерфейсы находятся в выделенном сегменте сети, доступ в данный сегмент ограничен					
15.	Для управления сетевым оборудованием используются только безопасные протоколы: SSHv2 разрешен, протокол Telnet запрещен.					
16.	На сетевых устройствах заблокированы стандартные привилегированные учетные записи					
17.	Применяются персонифицированные учетные записи для администрирования сетевого оборудования. Все учетные записи являются актуальными и используемыми					
18.	Применяется сервер AAA для доступа администраторов к сетевым устройствам. Настроены требования к паролям привилегированных учетных записей.					
19.	Резервное копирование конфигураций сетевых устройств					
Безопасность рабочих станций и серверов						
20.	Рабочие станции и сервера расположены в различных сегментах КСПД, отделены МЭ.					
21.	Серверные сегменты разделены по степени критичности сетевых служб, сегменты отделены МЭ					
22.	Доступ с серверов в сеть Интернет заблокирован. Разрешены минимально необходимые подключения для функционирования серверных компонентов					
23.	Сегменты пользовательского доступа разделены на основе функциональных обязанностей и критичности предоставленных доступов					

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
24.	Задействован механизм аутентификации устройств на уровне сети (802.1x)					
25.	Механизмы защиты сети на канальном уровне: DHCP-Snooping, Dynamic ARP Protection, Dynamic IP Lockdown и т.д.					
26.	Отключение автоматического определения режима порта коммутатора (access/trunk)					
27.	Сетевой доступ между рабочими станциями заблокирован					
Безопасность инфраструктуры Windows						
28.	Аутентификация пользователей на Windows-серверах и рабочих станциях осуществляется по учетным записям Active Directory. Локальные учетные записи ОС отключены					
29.	Разделение привилегированных УЗ с различным уровнем административных полномочий: «Администратор домена», «Администратор сервера», «Администратор раб. станций». Запрещено совмещение УЗ с различным уровнем административных полномочий. К примеру, запрещен вход на рабочие станции под УЗ «Администратор домена»					
30.	Задействована двухфакторная аутентификация для привилегированных УЗ инфраструктуры Windows					
31.	Запрещена аутентификация учетных записей Active Directory с применением небезопасных протоколов LM и NTLM. Разрешены протоколы NTLMv2 или Kerberos					
Антивирусная защита						
32.	Администрирование СЗИ на рабочих станциях и серверах должно осуществляться с использованием централизованного сервера управления					

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
33.	Должны быть назначены ответственные за администрирование СЗИ. Только данные сотрудники должны иметь права административного доступа к консоли управления СЗИ.					
34.	Антивирусные средства должны быть установлены на всех серверах и рабочих станциях, подверженных воздействию вредоносного ПО					
35.	Сигнатуры антивирусных средств должны обновляться не реже одного раза в день. Обновление сигнатур должно осуществляться с использованием централизованного сервера управления					
36.	На антивирусных средствах должно быть включено ведение журналов событий. Журналы событий должны передаваться на централизованный сервер					
37.	Должен контролироваться состав установленного ПО на рабочих станциях и серверах с помощью антивирусных средств или иного специализированного ПО					
Безопасность систем дистанционного банковского обслуживания						
38.	ПО систем «Банк-Клиент» установлено на отдельную, специально выделенную рабочую станцию					
39.	Антивирусная защита рабочих станций, на которых установлено ПО «Банк-Клиент», замкнутая программная среда, ограничение разрешенных УЗ, контроль съемных устройств, двухфакторная аутентификация в ОС,					

№	Критерий оценки	Результат	Тип проведенных проверок	Текущая ситуация	Недостатки, уязвимости и угрозы	Рекомендации по устранению угроз
40.	Рабочие станции, на которых установлено ПО «Банк-Клиент, выведены в отдельный сегмент сети, межсетевое взаимодействия ограничено минимальным набором правил, доступ в сеть Интернет ограничен списком разрешенных IP-адресов					
41.	Утверждена политика ИБ систем «Банк-Клиент», инструкция оператора, технический паспорт					
Настройки аудита						
42.	Регистрация событий на сетевом оборудовании и инфраструктурных серверах (DC, DNS, DHCP и т.д.)					
43.	Наличие выделенного хранилища логов					

При анализе конфигураций компонент ИТ-инфраструктуры необходимо указывать в листе проверок (Check List) параметры и атрибуты анализируемых компонент (ip-адреса, доменные имена, названия устройств и т.д.).

В случае необходимости проанализировать специфический компонент ИТ-инфраструктуры, для которого отсутствуют критерии в Check List, критерии формируются в процессе аудита по решению аудитора ИБ.

5. Оценка существующей реализации процессов управления ИБ

Целью данного этапа является оценка зрелости системы управления ИБ на основе информации о существующих процессах управления ИБ.

Выявление недостатков в процессах управления ИБ является необходимым условием для совершенствования системы обеспечения ИБ Компании.

Результаты аудита процессов управления ИБ позволяют разработать корректирующие мероприятия по совершенствованию системы обеспечения ИБ путем внедрения организационных мер (частных политик ИБ, регламентов, стандартов, процедур и т.д.).

Аудиту подвергаются следующие процессы ИБ:

- управления доступом к ИС/ИР;
- управления уязвимостями и установкой обновлений ПО;
- управления изменениями;
- регистрации и мониторинга событий ИБ;
- управления инцидентами ИБ;
- повышения осведомленности сотрудников по вопросам ИБ.

В рамках данного этапа заполняется контрольный лист «Оценка базовых процессов

ИБ» (Таблица 3).

Таблица 3

Контрольный лист «Оценка базовых процессов ИБ»

№	Название документа	Результат	Описание текущей ситуации	Недостатки и уязвимости	Рекомендации к улучшению
Управление доступом к ИС/ИР					
1.	Регламентирована и реализована формальная процедура предоставления, изменения и отмены доступа внутренних и внешних пользователей				
2.	Документирован реестр информационных систем и ресурсов, для каждого ресурса установлен владелец, администратор безопасности, системный администратор				
3.	Документированы типовые должности и роли сотрудников и соответствующие им права доступа в системах				
4.	Сотрудникам назначаются индивидуальные учетные записи для доступа к системным компонентам. Запрещено совместное использование учетных записей в системах				
5.	Проводится периодический пересмотр прав доступа сотрудников для выявления неиспользуемых прав доступа. Результаты пересмотра документируются				
6.	Используются средства централизованного контроля доступа к информационным ресурсам				
Управление уязвимостями и установкой обновлений ПО					
7.	Регламентирована и реализована формальная процедура выявления и документирования уязвимостей используемого ПО и сетевых протоколов, а также принятия мер по нейтрализации уязвимостей				
8.	Документирован перечень используемого ПО и сетевых протоколов, для которых осуществляется мониторинг уязвимостей				

№	Название документа	Результат	Описание текущей ситуации	Недостатки и уязвимости	Рекомендации к улучшению
9.	Для получения информации об уязвимостях используются достоверные внешние источники				
10.	Для выявленных уязвимостей проводится оценка рисков, на основании которой определяется критичность уязвимостей, а также принимаются решения о необходимых мерах по их нейтрализации. Результаты оценки рисков и решения о необходимых мерах документируются				
11.	Ведется реестр выявленных уязвимостей, включающий в себя их степень критичности и состояние реализации мер по их устранению				
12.	Проводится периодическая инвентаризация узлов сети с целью обеспечения полноты сканирования ИТ-инфраструктуры на наличие уязвимостей				
13.	Проводится регулярное сканирование уязвимостей информационных систем и сетевого оборудования				
Управление изменениями					
14.	Регламентирована и реализована формальная процедура инициирования, согласования и документирования изменений в ИТ-инфраструктуре				
15.	Для всех изменений в ИТ-инфраструктуре производится оценка рисков ИБ и разрабатываются необходимые меры по их снижению				
16.	Регламентированы требования к составу и содержанию технической документации по информационной инфраструктуре. Документация актуальна и соответствует требованиям.				
Регистрация и мониторинг событий ИБ					
17.	Регламентирована и реализована формальная процедура мониторинга событий ИБ				

№	Название документа	Результат	Описание текущей ситуации	Недостатки и уязвимости	Рекомендации к улучшению
18.	Документированы требования к регистрации системных событий ИС, включая регистрацию действий пользователей и администраторов, изменений системных настроек, а также события аутентификации и авторизации. Требования включены в стандарты настройки систем. Системные компоненты настроены в соответствии со стандартами настройки				
19.	Документированы требования к местам, формам и срокам хранения журналов системных событий информационных ресурсов. Журналы хранятся в соответствии с требованиями				
20.	Документированы требования к обеспечению синхронизации системного времени информационных систем. Требования включены в стандарты настройки систем. Системные компоненты настроены в соответствии со стандартами настройки				
21.	Внедрены технические средства мониторинга событий ИБ				
22.	Определены типы событий, о которых должен оповещаться персонал, ответственный за мониторинг событий ИБ. Технические средства мониторинга событий настроены соответствующим образом				
Управление инцидентами ИБ					
23.	Регламентирована и реализована формальная процедура реагирования на инциденты ИБ и их расследования				
24.	Определены критерии идентификации, типы и классификация инцидентов ИБ				
25.	Разработаны планы реагирования на инциденты ИБ				
26.	Проводится регулярное тестирование планов реагирования на инциденты ИБ				

№	Название документа	Результат	Описание текущей ситуации	Недостатки и уязвимости	Рекомендации к улучшению
27.	Анализ причин инцидента и внесение изменений в систему ОИБ				
Повышение осведомленности сотрудников по вопросам ИБ					
28.	Разработана учебная программа повышения осведомленности сотрудников в вопросах ИБ, учитывающая специфику работы различных групп сотрудников				
29.	Обучение сотрудников по вопросам ИБ проводится периодически, а также проводятся первичные инструктажи при приеме на работу, ведется журнал инструктажа				
30.	Тестирование знаний сотрудников в вопросах ИБ по итогам обучения проводится периодически, а также при приеме на работу.				
31.	Разработаны инструкции для сотрудников, определяющие требования ИБ, определена ответственность за нарушение требования ИБ. Сотрудники ознакомлены с инструкциями под подпись				

6. Проведение инструментальных проверок

Целью данного этапа является практическая демонстрация угроз ИБ, выявленных на предыдущем этапе «Оценка сетевой инфраструктуры и применяемых средств и мер ИБ».

Инструментальный анализ заключается в проведении аудитором ИБ совместно с сотрудниками Компании проверок исследуемых информационных систем и средств защиты информации с применением специализированного программного и аппаратного обеспечения.

Настоящая Методика не включает анализ защищенности компонентов ИТ-инфраструктуры посредством активной эксплуатации уязвимостей по принципу «Черный ящик». Инструментальные проверки формируются на основе данных, полученных на предыдущих этапах аудита.

В контексте настоящей Методики инструментальный анализ состоит из двух частей:

- контроль и анализ информационных потоков в ИТ-инфраструктуре (преимущественно на периметре корпоративной сети передачи данных) с целью выявления угроз ИБ, исходящих от внутренних пользователей (сотрудников) Компании или с целью выявления скомпрометированных компонентов ИТ-инфраструктуры;

- анализ защищенности компонентов ИТ-инфраструктуры с целью выявления уязвимостей программного и аппаратного обеспечения посредством сканирования систем на уровне сети.

6.1. Контроль и анализ информационных потоков

Данный вид инструментальных проверок проводится с применением специализированного программного обеспечения, осуществляющего анализ трафика, проходящего через периметры корпоративной сети передачи данных. Результатом анализа является:

- определение приложений высокого уровня риска, запускаемых периодически и функционирующих на постоянной основе на рабочих станциях и сервера;
- определение web-сайтов сомнительного характера, используемых сотрудниками: пиринговых сетей, облачных файловых хранилищ, прокси и анонимайзеров, вредоносных сайтов и т.д.
- обнаружение рабочих станций и серверов, инфицированных вредоносным программным обеспечением и/или являющихся частью бот-сетей.
- оценка уязвимостей серверов и компьютеров компании, являющихся целью возможных атак;
- анализ полосы пропускания и идентификация наиболее ресурсоемких приложений и веб-сайтов: кто и каким образом более всего загружал сеть;
- дополнительно может быть проведен анализ входящего SMTP-трафика с целью обнаружения вредоносного программного обеспечения, распространяемого в рамках попыток проведения целенаправленных атак.

Обследование ИТ-инфраструктуры предусматривает установку шлюза безопасности с установленным специализированным программным обеспечением внутри сети. Инспектируется копия трафика за счет подключения к соответствующему устройству Test Access Point (ТАР) или порту зеркалирования на сетевом коммутаторе. Ниже представлена схема подключения:

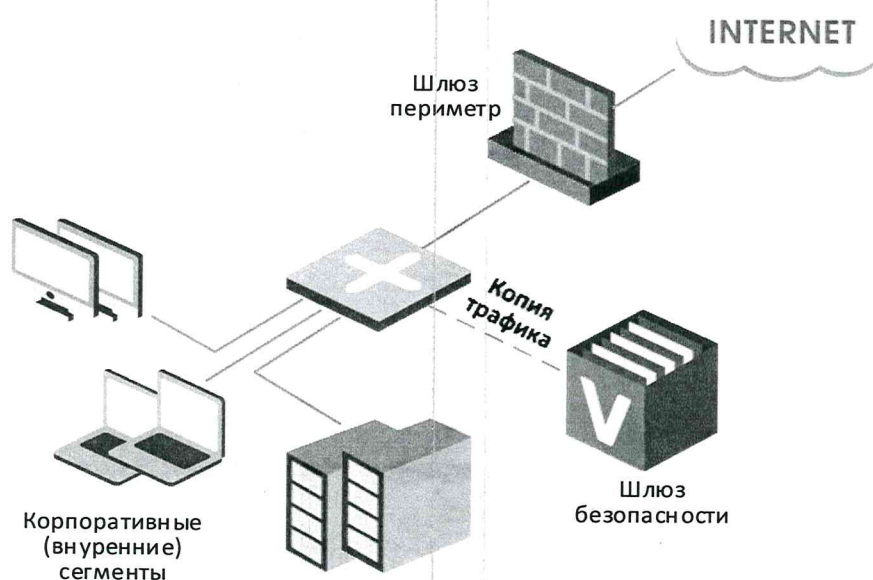


Рис. 2. Схема подключения шлюза безопасности.

6.2. Анализ защищенности компонентов ИТ-инфраструктуры

В рамках данной инструментальной проверки осуществляется автоматическое сканирование узлов корпоративной сети на наличие уязвимостей операционной системы и прикладного ПО, а также сетевого оборудования. Тестирование компонентов инфраструктуры Windows осуществляется с минимальными и максимальными привилегиями по отношению к тестируемой системе. При этом используется: расширенная проверка нестандартных портов, баннерные проверки сетевых служб, идентификация типов и версий сетевых служб и приложений по особенностям протоколов, проверка стойкости паролей учетных записей.

Анализ защищённости проводится: в целях оценки возможности преодоления потенциальным нарушителем системы защиты ИТ-инфраструктуры и нарушения ее безопасного функционирования за счет эксплуатации уязвимостей программного обеспечения и оборудования; проверки соответствия настроек программного обеспечения и оборудования требованиям по информационной безопасности Компании.

В рамках анализа защищенности проводится:

- сканирование рабочих станций и серверов, расположенных во внутренних сегментах корпоративной сети передачи данных (далее КСПД);
- сканирование сетевого оборудования КСПД;
- сканирование внешнего периметра, в том числе на наличие доступных из сети Интернет сервисов.

Анализ защищенности проводится с применением специализированного программного обеспечения: сканер защищенности, сканер IP-сетей, определяющий состояния портов и соответствующих им служб.

7. Анализ выявленных уязвимостей и недостатков и связанных с ними угроз

Результатом аудита безопасности ИТ-инфраструктуры Компании являются:

- оценка эффективности применяемых средств и мер защиты информации;
- оценка реализации процессов ИБ;
- выявленные уязвимости и связанные с ними угрозы;
- выявленные недостатки мер защиты и связанные с ними угрозы.

Эффективность применяемых средств и мер защиты информации и реализация процессов ИБ оцениваются количественным показателем в диапазоне от 0 до 5.

Оценки определяются методом экспертного заключения и не основываются на каких-либо распространенных стандартах.

Для наглядного представления результатов оценки показатели эффективности применяемых средств и мер защиты информации, а также оценки реализации процессов ИБ отображаются на диаграмме и заносятся в таблицу. Примеры диаграмм и структура таблиц приведены ниже.

7.1. Перечень средств и мер защиты информации, для которых выставляется оценка, включает:

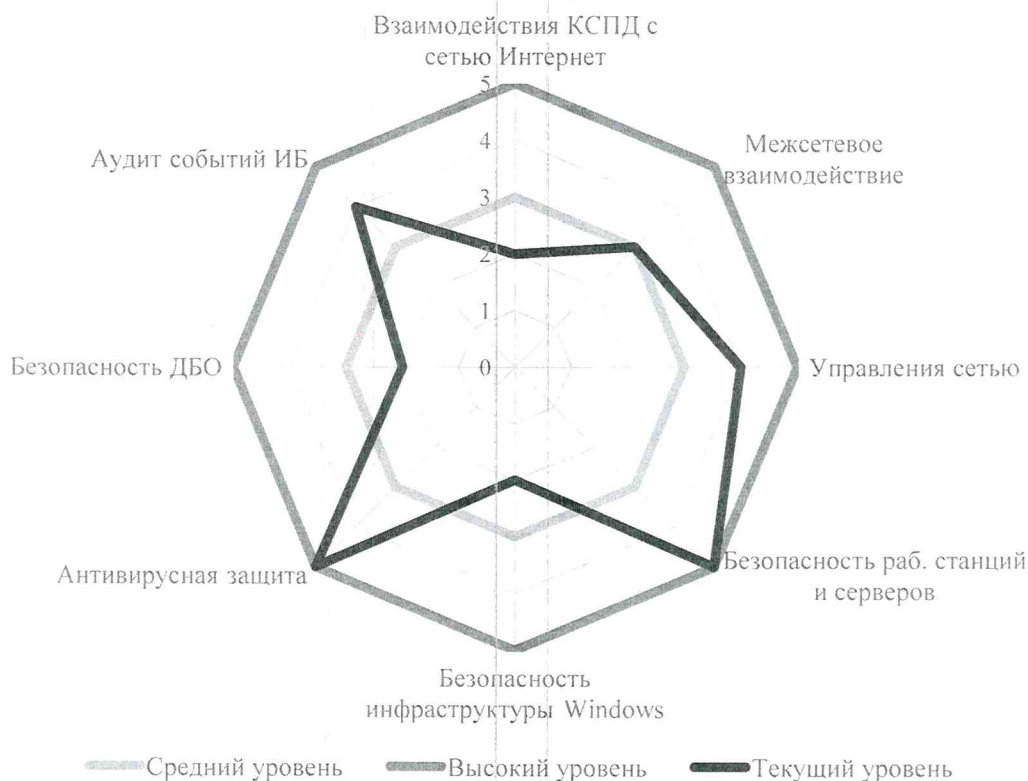


Рис.3 Диаграмма эффективности средств и мер защиты информации.

Таблица 4

Оценка эффективности мер и средств защиты информации

№ п/п	Меры обеспечения информационной безопасности	Описание	Оценка (от 0 до 5)
1	Безопасность взаимодействия КСПД с сетью Интернет		
2	Безопасность межсетевого взаимодействия (между сегментами КСПД)		
3	Безопасность управления сетью		
4	Безопасность рабочих станций и серверов		
5	Безопасность инфраструктуры Windows		
6	Антивирусная защита рабочих станций и серверов		
7	Безопасность систем ДБО		
8	Аудит событий ИБ		
Заключение			

7.2. Оценке подлежит реализация следующих процессов ИБ:

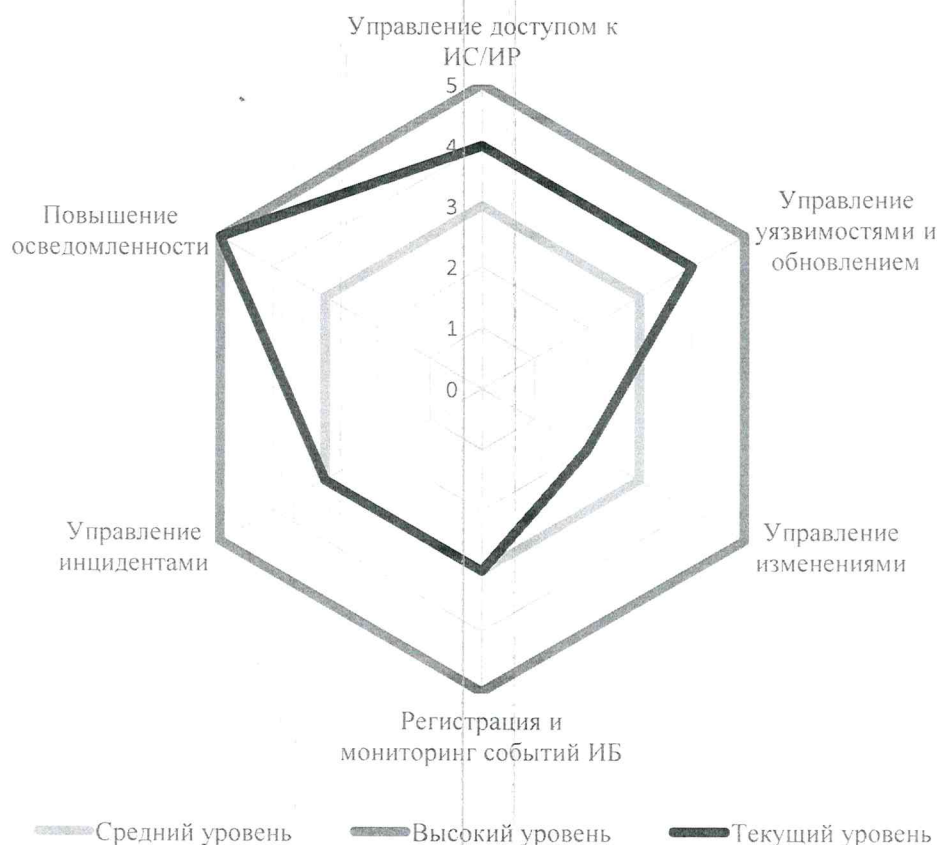


Рис. 4. Диаграмма эффективности реализации процессов ИБ.

Таблица 5

Оценка эффективности мер и средств защиты информации

№ п/п	Процессы ИБ	Описание	Оценка (от 0 до 5)
1	Управление доступом к ИС/ИР		
2	Управление уязвимостями и установкой обновлений ПО		
3	Управление изменениями		
4	Регистрация и мониторинг событий ИБ		
5	Управление инцидентами ИБ		
6	Повышение осведомленности сотрудников по вопросам ИБ		
Заключение			

7.3. Выявленные уязвимости и связанные с ними угрозы

В ходе анализа результатов инструментальных проверок указываются выявленные уязвимости, которые могут привести к возникновению угроз бизнес-процессам Компании. Производится экспертная оценка уровня критичности угрозы в зависимости от обнаруженной уязвимости. Данные заносятся в таблицу (Таблица 6).

Таблица 6

Выявленные уязвимости и связанные с ними угрозы

№ п/п	Обнаруженная уязвимость	Угроза бизнес-процессам Компании	Уровень критичности
1			
2			
3			
4			

7.4. выявленные недостатки мер защиты и связанные с ними угрозы

В результате оценки реализованных защитных мер в сетевой инфраструктуре фиксируются недостатки, которые могут привести к возникновению угроз бизнес-процессам Компании. Производится экспертная оценка уровня критичности угрозы в зависимости от обнаруженного недостатка. Данные заносятся в таблицу (Таблица 7).

Таблица 7

Выявленные недостатки защитных мер сетевой инфраструктуры.

№ п/п	Обнаруженный недостаток	Угроза бизнес-процессам Компании	Уровень критичности
1			
2			
3			
4			

В таблице 8 приведена классификация уровней критичности угроз, соответствующих выявленным недостаткам мер защиты и уязвимостям.

Таблица 8

Уровни критичности угроз

Уровень критичности	Описание
Высокий	Наличие недостатка или уязвимости влияет напрямую на безопасность критичных данных или систем. Возможно получение доступа к критичным данным при помощи эксплуатации уязвимости
Средний	Наличие недостатка или уязвимости напрямую не влияет на безопасность критичных данных. Получение доступа к критичным данным за счет эксплуатации уязвимости или в результате недостатка мер защиты невозможно. Однако возможно получение такого доступа в случае наличия либо возникновения и эксплуатации прочих уязвимостей совместно с данной
Низкий	Наличие уязвимости или недостатка не влияет на безопасность критичных данных. Возможность получения доступа к критичным данным значительно затруднена либо отсутствует

При необходимости количественной оценки производится расчет риска в зависимости от ценности актива бизнес-процесса Компании, выявленных недостатков, уязвимостей и угроз. Расчетное значение может применяться для выбора и обоснования внедрения необходимых средств защиты.

Лист регистрации изменений

Порядковый номер изменения	Основание ¹	Срок введения изменения	Изменения внес			Примечания
			ФИО	Подпись	Дата внесения изменения	

¹ Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.