МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Тольяттинский государственный университет
(наименование института полностью)

Кафедра Прикладная математика и информатика
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Управление корпоративными информационными процессами
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Модели и методы системы обеспечения информационной безопасности предприятия

Обучающийся К.О. Мухин _____
(Инициалы Фамилия) (личная подпись)

Научный руководитель: канд. пед. наук, доцент О.В. Оськина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Оглавление

Введение

Информационные системы глубоко проникли в структуры современного общества. И сегодня уже невозможно представить функционирование какой-либо сферы нашей жизни без них. Информация в настоящее время является важным ресурсом. И как только увеличилась ценность информации, так сразу возросла заинтересованность в ней и, соответственно, угроза ее безопасности.

Характерной особенностью современных информационных атак является не требование денежного выкупа, а стремление помешать работе бизнеса.

Внедрение информационных технологий обуславливает как положительные изменения в развитии общества, так вызывает и множество различных проблем. Рост информационных сетей приводит к увеличению конкуренции, числу пользователей, а также и к несанкционированному доступу к хранящейся и передающейся в этих сетях информации. Фальсификация информации или незаконное ее искажение, а также разглашение всей информации или какой-либо ее части могут нанести серьезный моральный и материальный ущерб как репутации предприятия, так и его финансовому положению.

Разработка эффективных моделей системы обеспечения информационной безопасности предприятия в совокупности с современными методами защиты представляет актуальность и научно-практический интерес.

Целью работы является исследование методов и разработка моделей для повышения информационной безопасности предприятия.

Объектом исследования является система обеспечения информационной безопасности предприятия.

Предметом исследования являются модели и методы системы обеспечения информационной безопасности предприятия.

В структуре информационной безопасности действуют довольно жесткие требования к защите данных. И эти требования расширяются и усиливаются в

соответствии с совершенствованием и развитием технологий осуществления угроз безопасности.

В АО «Нител» регулятором текущего состояния защищенности информации и информационных структур предприятия является федеральная служба по техническому и экспертному контролю (ФСТЭК).

Фактическое исследование состояния технической защиты информации по Методике оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (Методика), представленной ФСТЭК, показало, что на предприятии отсутствует минимальный уровень защищенности информации от актуальных угроз и имеется объективная возможность их реализации [13].

Гипотезой исследования является комплексное применение новых актуальных моделей защиты данных, в основе которых лежат современные методы, обеспечат повышение информационной безопасности предприятия.

Для решения поставленных задач необходимо:

- изучить структуру информационной сети предприятия и функционирующую в этой сети информацию;
- проанализировать существующие в информационной сети уязвимости;
- разработать необходимые модели и выбрать методы и средства для обеспечения информационной безопасности, соответствующие современному уровню развития технических средств;
- провести оценку состояния информационной безопасности после проведения всех запланированных мероприятий.

Теоретическая значимость исследования состоит в изучении новых методов и моделей защиты данных в информационной сети, позволяющих значительно повысить защиту информации.

Практическая значимость работы определяется тем, что ее результаты позволят повысить степень защищенности информации на предприятии путем использования разработанных моделей и предложенных методов, направленных

на снижение информационных рисков, безопасного применения цифровых технологий.

Научная новизна исследования заключается в:

– формировании защищенного доступа к общедоступной и служебной информации для ведущих специалистов в общей сети предприятия;
– разработке и апробации модели оценки безопасности установки обновлений иностранного программного обеспечения, используемого на предприятии.

В основе теоретического исследования лежат нормативно-правовые документы, регулирующие сферу защиты информационной безопасности в организациях, исследования в области защиты информации.

Основное исследование проводились с 2023 по 2025 год в несколько этапов.

На первом этапе формулировалась тема исследования, проводился сбор информации из различных источников, осуществлялась формулировка гипотезы, постановка цели, задач.

В ходе второго этапа были проведены исследование информационной системы предприятия и оценка ее защищенности согласно Методике [13].

Третий этап заключается в модернизации существующих или разработке новых моделей и методов обеспечения информационной безопасности предприятия, их апробации и внедрении в действующую систему безопасности, по итогам выполненных задач - повторной оценке показателя защищенности информации и оценке эффективности проведенной работы.

На защиту выносятся:

– модели, разработанные для обеспечения информационной безопасности предприятия;
– результаты апробации и оценка эффективности предлагаемых решений.

Магистерская диссертация состоит из введения, пяти глав, заключения, списка используемой литературы и используемых источников.

В первой главе проведен анализ проблемы защиты информационной сети, рассмотрены необходимость и актуальность сохранности информации в настоящее время, раскрыты сущность и цели информационной безопасности. Обоснована необходимость комплексной организации системы защиты на предприятии.

Вторая глава посвящена исследованию информационной системы предприятия и оценке ее защищенности по Методике. По результатам «оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры» [13, п. 36] сделан вывод о необходимости разработки необходимых мероприятия для повышения показателя надежности.

В третьей главе проанализирована структура информационной системы и рассмотрены виды информации, существующие в данной системе, на основе ролевой политики доступа и модели внутреннего нарушителя информационной безопасности сформирована матрица разграничения доступа к служебной информации для ведущих сотрудников предприятия и обосновано применение двухфакторной аутентификации для них. В данном разделе обоснована необходимость введения в политику безопасности предприятия Регламента реагирования на инциденты информационной безопасности и рассмотрены основные этапы ее разработки.

В четвертой главе разработана, исследована и апробирована модель оценки безопасности установки обновлений иностранного программного обеспечения во избежание их негативных последствий на информационную систему предприятия, проведена оценка эффективности ее разработки.

В пятой главе рассчитаны экономические затраты предприятия, обусловленные выполнением мероприятий для повышения состояния технической защиты информации, проведена и проанализирована повторная оценка показателя защищенности.

Работа изложена на 76 страницах и включает 10 таблиц, 25 рисунков и 36 источников.

Глава 1 Анализ проблемы защиты информации в компьютерной сети предприятия

В современном обществе информация представляет собой продукт, который можно купить, продать или просто обменять. И цена такого продукта иногда многократно превышает стоимость самой автоматизированной системы, которая хранит и обрабатывает эту информацию. «Устойчивое функционирование и развитие промышленных предприятий в эпоху четвертой промышленной революции напрямую зависит от надежного и безопасного применения цифровых технологий, в том числе автоматизации и систем управления производственными процессами» [28].

Согласно ГОСТ Р 50922-2006, под защитой информации понимается «деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию» [16, п. 2.1.1].

В большинстве случаев краже подвергаются данные о фактическом финансовом положении предприятия, новых научных и технических разработках, учетные данные пользователей для доступа к серверам и персональные данные сотрудников. Утечка данных может отрицательно сказаться на деятельности предприятия не сразу после ее осуществления, а спустя некоторое время. Украденная интеллектуальная собственность может снизить рентабельность компании и подорвать ее конкурентные преимущества [34]. И от степени защиты этой информации зависят стабильность работы предприятия, сохранность финансов и его репутация. Как говорит в своей статье В.Д. Рычков «информационная безопасность уже по определению защищается, а значит, нападающие всегда на шаг впереди, как минимум в своих преступных намерениях. Это, собственно и есть проблема №1 – понять сам факт необходимости мероприятий по ИБ для организации» [23].

По данным центра мониторинга и реагирования на кибератаки RED Security количество кибератак за 2024 год по сравнению с 2023 годом выросло в

2,5 раза и достигло 130 тысяч случаев. Самая атакуемая отрасль – промышленность, на предприятия из отраслей критической инфраструктуры пришлось около 64 % от общего числа инцидентов за год [29]. При этом количество высококритичных атак, которые могли бы привести к потерям компаний или паузе в их работе, за прошедший год составило около 26 тысяч случаев.

«Защита информационной инфраструктуры в 2025 г. становится еще более многогранной задачей, требующей комплексного подхода. С одной стороны, организации должны продолжать адаптироваться к ужесточению требований регуляторов, активно внедрять механизмы импортозамещения и соблюдать новые стандарты защиты инфраструктуры. С другой стороны, вызовы, такие как развитие атак с использованием искусственного интеллекта и уязвимость цепочек атак, требует внедрения более эффективных средств защиты информации и совершенствования методов управления рисками» [24].

Абсолютная защита информации практически невозможна, т.к. в любой системе велика вероятность человеческой ошибки. На предприятии защита информации обеспечивается только на период времени, пока несанкционированный допуск к ней влечет какие-либо последствия, т.е. защита информации является относительной. Это означает, что конфиденциальная информация должна быть недоступна до того момента, пока она станет либо очевидной и понятной, либо никому не нужной. Оптимальным уровнем защиты информации на предприятии является такой, при котором себестоимость атаки выше, чем вероятная экономическая выгода злоумышленника.

«Всю суть защиты информации можно свести к одной цели – необходимо обеспечить безопасность всех элементов любого элементарного информационного потока в каждый момент времени» [6].

Безопасность информации определяется состоянием ее защищенности, обеспечивающим конфиденциальность, доступность и целостность, которые являются ее основными свойствами и равнозначны по отношению к гарантии ее безопасности [20].

Конфиденциальность информации подразумевает ее доступность только пользователю, имеющему к ней санкционированный доступ, и не может быть использована посторонними лицами [32].

Целостность гарантирует сохранность информации и ее свойств. Доступность предполагает, что информация доступна конкретному пользователю для использования в необходимые время и место.

При правильно разработанной и организованной системе безопасности информация невосприимчива к случайным или умышленным воздействиям, стремящимся нарушить ее целостность, доступность и конфиденциальность.

Организация безопасности на предприятии должна быть основана на таких принципах, как системность, многоуровневость защиты, прочность, благоразумность и бесперебойность. Такой подход означает то, что информационная безопасность должна обеспечивать исключение информационных атак со стороны внешних и внутренних нарушителей. Средства защиты должны технически дополнять друг друга, обладать многоуровневой структурой, включающей в себя несколько последовательно расположенных зон безопасности, главная из которых будет находиться внутри всей системы. Зоны безопасности должны иметь одинаковый уровень защиты с возможностью идентификации угроз. Функционирование информационной безопасности должно быть надежным и бесперебойным. Применяемые защитные меры должны обеспечивать необходимую и гарантированную степень безопасности информации на предприятии. Как пишет Ю.А. Гатчин «наибольший эффект может быть достигнут только в том случае, когда все используемые средства, методы и меры объединяются в единый целостный механизм - комплексную систему защиты информации. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий» [2, с.15].

На сегодняшний день организационная структура предприятия очень сложная, т.к. она обладает многофункциональностью, высокой технической

оснащенностью, большими объемами поступающей, обрабатываемой и хранящейся информации. Предприятие осуществляет свою деятельность в условиях самых разнообразных угроз информационной безопасности.

Угроза безопасности информации – это «совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации» [16, п. 2.6.1].

На предприятии для всех информационных ресурсов необходимо обеспечить определенный уровень конфиденциальности, целостности и доступности, поэтому целесообразно акцентировать внимание на предотвращение таких угроз, как угроза доступности, угроза конфиденциальности и угроза целостности [14].

Угрозами доступности могут быть непреднамеренные ошибки пользователей, персонала, обслуживающего информационные сети. Например, неправильно введенные данные приводят к сбою программного обеспечения, и допущенная при этом неточность администратора подвергает риску всю систему. Около 65% потерь информации происходит именно из-за непреднамеренных просчетов [27]. «Отклонение может произойти в источнике (из-за невозможности для сервера получить ресурсы, необходимые для выполнения его функций), в пункте назначения (из-за блокировки связи с сервером) или на промежуточном пути (из-за отбрасывания сообщений либо от клиента, либо от сервера, либо от обоих)» [35].

Угроза нарушения конфиденциальности заключается в раскрытии конфиденциальной или секретной информации, т.е. информация, существующая в корпоративной сети, становится доступной лицам, которые не имеют к ней доступ.

Угроза нарушения целостности информации, которая функционирует в компьютерной сети предприятия, проявляется в изменении или полном искажении информации, что приводит к нарушению ее качества или уничтожению [9].

Стремительное развитие информационных технологий привело к тому, что современные программные продукты попадают на рынок без достаточной отработки и отладки. Эти ошибки и недоработки программного обеспечения провоцируют возникновение уязвимостей в сетях предприятия и являются причинами реализации угроз безопасности. Уязвимости существуют в любой информационной системе, неразрывны с ней, потому что зависят от несовершенства механизма функционирования и архитектуры этой информационной системы, интерфейса и реализуемыми протоколами обмена, условиями эксплуатации и т.д.

В среднем соотношение внешних и внутренних угроз выглядит так:

- 82 % угроз – это внутренние угрозы, которые реализуются при прямом или косвенном участии самими сотрудниками предприятий;
- 17 % – это внешние угрозы, они совершается извне;
- 1 % угроз совершается случайными лицами [8].

Всякая угроза приводит к какому-либо ущербу, моральному или материальному. И величину данного ущерба призваны снизить защита от угрозы и противодействие ей, в идеальном случае – в полном объеме, в реальном – существенно или хотя бы частично, но это возможно далеко не всегда. Поэтому одна из основных задач защиты информации – необходимость точности определения уязвимостей и угроз информации, потенциально возможных в существующих информационных системах, потому что даже один неучтенный или непринятый во внимание дестабилизирующий фактор может значительно снизить эффективность защиты информационной системы.

В первой главе были рассмотрены цели и основные задачи информационной безопасности, проанализированы трудности защиты информации в настоящее время, определена необходимость комплексной организации системы защиты на предприятии.

Глава 2 Оценка текущего состояния системы безопасности информации

Для контроля предприятий в сфере организации информационной безопасности указами Президента определены федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) и федеральная служба безопасности Российской Федерации (ФСБ России).

Одними из основных задач ФСТЭК являются:

− «обеспечение в пределах своей компетенции безопасности значимых объектов критической инфраструктуры, противодействия техническим разведкам и технической защиты в организациях»;

− организация и проведение оценки «деятельности организаций по технической защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры» [26, п. 4].

Нормативные и правовые акты, разработанный ФСТЭК, обязательны для исполнения в АО «Нител».

Приказом ФСТЭК от 02.05.2024 была утверждена Методика, на основании которой на предприятии была проведена оценка текущего состояния защиты информации от типовых актуальных угроз безопасности информации [13].

Показателем текущего состояния защиты информации является показатель текущего состояния защищенности $К_{зи}$. Расчет данного показателя проводится не реже одного раза в 6 месяцев для всех информационных систем.

В Методике приведены четыре основные группы показателей, каждая из которых содержит свой весовой коэффициент. В каждой группе указаны частные показатели, характеризующие степень реализации отдельных мер по обеспечению безопасности от актуальных угроз. На рисунке 1 определены текущие значения частных показателей (K_{ji}) для групп 1 и 2, на рисунке 2 – для групп 3 и 4.

Номер группы показателей (i)	Наименование групп показателей	Наименование показателей	Значение частного показателя (Kji)	Значение весового коэффициента группы показателей (Rj)
1	Организация и управление	1.1 На заместителя руководителя организации возложены полномочия ответственного лица за обеспечение информационной безопасности организации и определены его обязанности	0,00	0,10
		1.2 Определены функции структурного подразделения, ответственного за обеспечение информационной безопасности организации	0,40	
		1.3 К подрядным организациям, имеющим доступ к информационным системам с привилегированными правами, в договорах установлены требования о реализации мер по защите от угроз через информационную инфраструктуру подрядчика	0,30	
2	Защита пользователей	2.1 Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике	0,30	0,25
		2.2 Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)	0,00	
		2.3 Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20	
		2.4 Отсутствуют активные учетные записи работников организации, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,00	

Рисунок 1 – Коэффициенты показателей надежности для групп 1 и 2

Номер группы показателей (i)	Наименование групп показателей	Наименование показателей	Значение частного показателя (Kji)	Значение весового коэффициента группы показателей (Rj)
3	Защита информационных систем	3.1 На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4	0,00	0,35
		3.2 На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня с датой публикации обновлений в банке угроз ФСТЭК России более 30 дней	0,20	
		3.3 На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновлений более 90 дней	0,10	
		3.4 Обеспечен документальный и автоматизированный учет пользовательских устройств, серверов и сетевых устройств	0,10	
		3.5 Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения	0,15	
		3.6 Обеспечено централизованное управление средствами антивирусной защиты. При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц	0,15	
		3.7 Реализована очистка входящего из сети Интернет входящего трафика от аномалий на уровне L3/L4 (заключен договор с провайдером)	0,10	
4	Мониторинг информационной безопасности и реагирование	4.1 Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,40	0,30
		4.2 Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35	
		4.3 Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,00	

Рисунок 2 – Коэффициенты показателей надежности для групп 3 и 4

На рисунке 3 показана диаграмма распределения показателей безопасности, разработанная по значениям частного показателя и их весового коэффициента, представленных на рисунках 1 и 2.

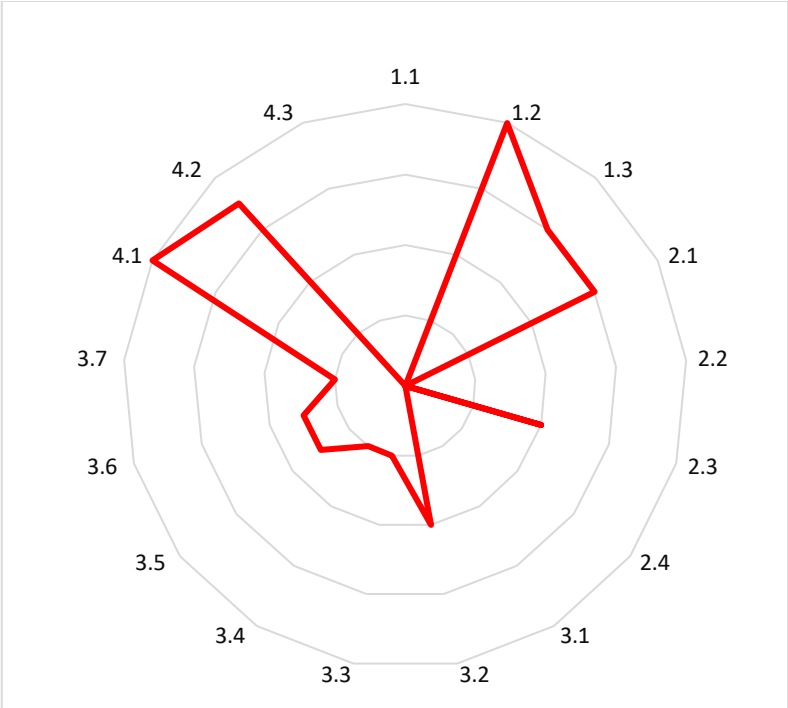


Рисунок 3 – Диаграмма распределения показателей безопасности по начальной оценке

Построение диаграммы наглядно показывает компоненты информационной структуры предприятия, по отношению к которым необходимо принять неотложные меры для повышения уровня информационной безопасности. Лучи диаграммы не должны иметь нулевых значений.

Расчет показателя надежности $К_{зи}$ осуществляется по формуле (1), используя значения частного показателя и значения весового коэффициента группы показателей, приведенных на рисунках 1и 2:

$$К_{ЗИ}=(k_{11}+k_{12}+k_{13})R_1+(k_{21}+\ldots+k_{2i})R2+(k_{31}+\ldots+k3_i)R3+(k_{41}+\ldots+k_{4i})R4 \qquad (1)$$

На рисунке 4 приведен график зависимости показателя текущего состояния защищенности ($К_{зи}$) от значения частных показателей (i).

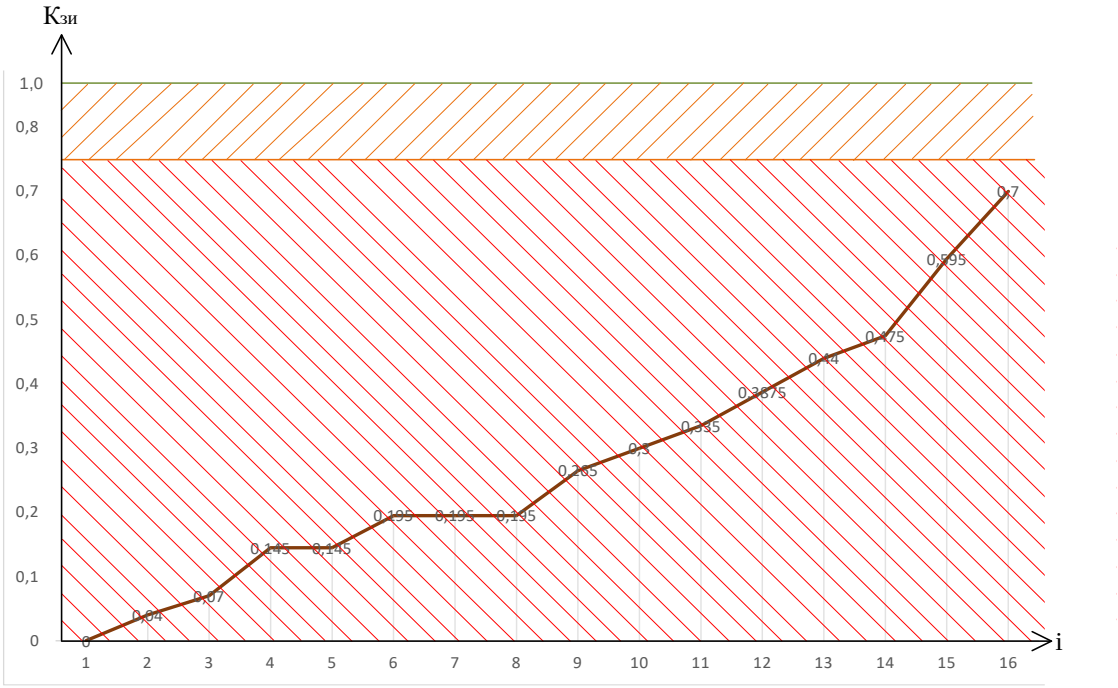


Рисунок 4 – График зависимости показателя текущего состояния защищенности от значения частных показателей

По результатам оценки текущего состояния информационной безопасности и проведенного расчета значение текущего состояния защищенности $К_{зи}$ (0,7) < 0,75, т.е. «минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень защищенности характеризуется как критический («красный»)» [13, п.35].

По результатам анализа состояния информационной безопасности было выявлено:

– отсутствие четкого административного управления информационной безопасностью на предприятии;

– отсутствие контроля учетными записями сотрудников;
– низкий уровень защиты от сетевых угроз на уровне распределения информации;
– отсутствие безопасного доступа к служебной информации для ведущих специалистов предприятия;
– отсутствие структурированного документа по реагированию на инциденты информационных угроз;
– неконтролируемая установка обновлений иностранного программного обеспечения.

Следовательно, необходимо «разработать план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз» [13, п. 36]. Для этого требуется исследовать информационную систему предприятия, проанализировать виды информации, существующие в сети, рассмотреть существующие модели безопасного доступа к данным и разработать новые, разработать модель тестирования обновлений операционной системы и регламент реагирования на инциденты информационной безопасности.

«При планировании способов достижения своих целей информационной безопасности организация должна определить:

– что должно быть сделано;
– какие ресурсы потребуются;
– кто будет нести ответственность;
– когда планируемое мероприятие будет завершено;
– как будут оцениваться результаты» [19, п.6.2].

Во второй главе на основе анализа структуры информационной системы предприятия была проведена оценка текущего состояния системы безопасности по Методике ФСТЭК. Математический и графический расчеты этой оценки показали, что на предприятии не обеспечивается минимальный уровень защиты информации от актуальных угроз и существует реальная возможность их реализации.

Глава 3 Усиление защиты информационной системы предприятия, способы реализации

3.1 Анализ существующих методов защиты информации и их использование для повышения информационной безопасности

Методы защиты информации на предприятии можно разделить на такие категории, как организационные (административные), технические (аппаратно-программные) и правовые.

Организационными являются меры и мероприятия, которые регламентируются внутренними положениями предприятия, эксплуатирующего информационную систему.

К правовым методам защиты информации относятся разработка и обновление положений нормативной базы по вопросам информационной безопасности и усиление контроля за их исполнением.

Технические методы основаны на использовании электронных устройств и специальных программ.

Для повышения текущего состояния информационной безопасности на предприятии необходимо:

- назначить ответственное за обеспечение информационной безопасности лицо и определить круг его обязанностей;
- обеспечить контроль учетных записей работников и их исключение при прекращении договорных или трудовых отношений;
- провести модернизацию технической защиты информационной системы предприятия на уровне распределения информации;
- обеспечить защищенный доступ ведущих специалистов к служебной информации;
- предусмотреть безопасность обновлений иностранного программного обеспечения;

– дополнить положения политики информационной безопасности.

Основные мероприятия и их ответственные исполнители показаны в таблице 1.

Таблица 1 – Мероприятия и исполнители

Мероприятие	Метод защиты информации	Ответственный
Разработка и оформление приказа о назначении ответственного лица за обеспечение информационной безопасности	организационный	начальник отдела безопасности
Обеспечение обмена между отделом информационной безопасности и отделом кадров	программный	сетевой администратор
Анализ сетевой инфраструктуры предприятия и выбор необходимых сетевых экранов	технический	специалист отдела безопасности, сетевой администратор
Разработка и организация защищенного доступа ведущих специалистов к служебной информации	организационно-программный	специалист отдела безопасности
Доработка программных модулей	программный	программист
Разработка модели тестирования обновлений иностранного программного обеспечения	программно-технический	программист, специалист отдела безопасности
Разработка Регламента реагирования на инциденты	организационный	специалист отдела безопасности

Выполнение первого пункта мероприятий – разработка приказа о назначении ответственного лица за обеспечение информационной безопасности на предприятии и определение его должностных полномочий входит в обязанности начальника отдела безопасности. Данное мероприятие полностью закрывается административными мерами.

Второй пункт мероприятий – контроль закрытия активных учетных записей работников организации, привлекаемых на договорной основе, с которыми прекращены трудовые или договорные отношения.

Данное мероприятие можно выполнить простым обменом информацией между службой безопасности и отделом кадров. При увольнении постоянных

сотрудников предприятия в соответствующем обходном документе делается отметка о закрытии учетной записи, а при расторжении трудовых договоров с временными сотрудниками такая форма обходного листа не предусмотрена. Решение данной проблемы можно обеспечить программным путем. На предприятии учет кадров осуществляется с помощью программы «1С: Зарплата и управление персоналом». Она предназначена для автоматизации кадрового учета, управления персоналом и расчетов с сотрудниками. В программе учета кадровых изменений оформляется прием и увольнение сотрудников, перевод их на другую работу и т.д. И на основе этой программы можно осуществлять рассылку отдела кадров о расторжении трудовых договоров в отдел информационной безопасности. Вид документа на увольнение, оформляемый отделом кадров на увольнение сотрудника, показан на рисунке 5.

После получения такого электронного документа на увольнение сотрудник информационного отдела имеет право закрыть соответствующую учетную запись.

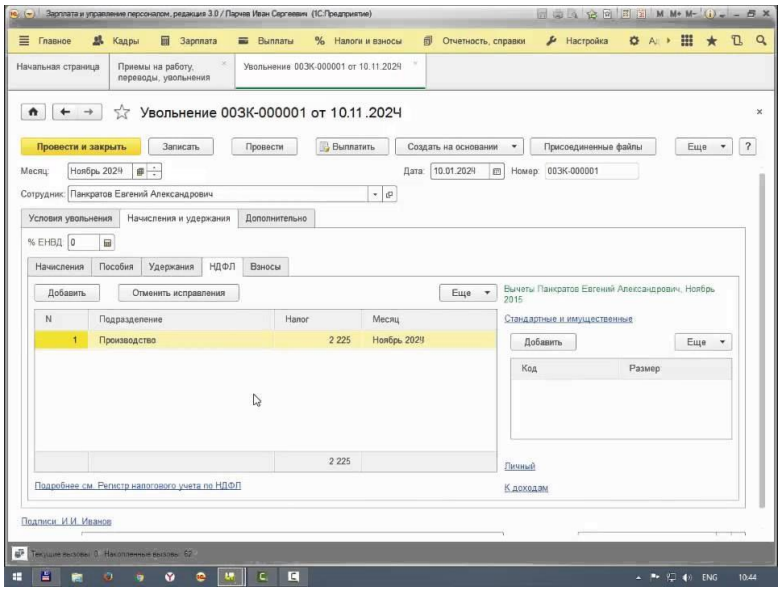


Рисунок 5 – Электронный документ на увольнение сотрудника

Для выполнение остальных мероприятий необходимо:

– провести анализ информационной системы предприятия;
– применить современные модели доступа к информации, существующей в сети предприятия, или разработать новые;
– разработать модель тестирования обновлений иностранного программного обеспечения;
– в политику безопасности ввести новое положение - документ о порядке реагирования на компьютерные инциденты.

3.2 Анализ информационной системы предприятия, повышение ее защищенности

Основные методы защиты информации предназначены для противодействия внешним угрозам. Но сейчас на предприятии остро встала задача противостояния инсайдерским атакам – защите от преднамеренных действий сотрудников предприятия, имеющих разрешенный доступ к информации. Безопасность от этих воздействий формируется:

– разграничением доступа в информационных системах;
– защитой информации при передаче ее по каналам связи;
– защитой от утечек информации по различным каналам;
– защитой от разрушающего воздействия вредоносного программного обеспечения (вирусов, троянских программ, программ-шпионов и т.д.);
– «материалами и средствами, обеспечивающие безопасность хранения, транспортировки ключей информации и их защиту от копирования» [20, с. 61].

Архитектура информационной сети предприятия разделена на несколько уровней. Каждый является уровень функционально законченной группой оборудования для выполнения определенных функций. Структура сети включает в себя уровень ядра, уровень распределения, уровень доступа и серверную ферму.

На уровне доступа к корпоративной сети подключены автоматизированные рабочие места, сетевые многофункциональные устройства и другие периферийные устройства. Оборудование данного уровня должно обеспечивать безопасность подключения пользователя к сети. На уровне доступа формируется сетевой трафик и выполняются контрольные функции, также устройства этого уровня определяют доступ пользователей к сети предприятия. Регулирование доступа к информационным ресурсам состоит из:

- идентификации пользователей, персонала и компьютерных ресурсов сети передачи данных;
- аутентификации - приема распознавания подлинности пользователя по идентификатору, указанному при входе в систему;
- контроля полномочий, т.е. проверки соответствия рабочих интервалов и запрашиваемых процессов установленным регламентом по времени и доступу;
- фиксирования всех запросов к защищаемым ресурсам и т.д. [17], [19].

Уровень распределения предназначен для распределения трафика абонентам. На этом уровне должно быть обеспечено резервирование и распределение нагрузки между соединениями. В настоящее время на уровне распределения стоят управляемые коммутаторы уровня L2. Эти коммутаторы реализуют проверку трафика между разными сетями и узлами, но для защиты информационной системы от сетевых угроз они недостаточно эффективны. Для повышения уровня информационной безопасности на уровне сегментации сети их необходимо заменить на коммутаторы уровня L3/ L4. Коммутаторы этого уровня контролируют доступ к сети, защищают от перегрузок, несанкционированного доступа, распространения вирусов и др. Для модернизации информационной системы выбран маршрутизатор Eltex ESR-100-st, сертифицированный ФСТЭК.

По всем предъявленным параметрам выбранное устройство легко встроится в информационную систему предприятия и обеспечит все необходимые параметры для ее защиты.

Встраиванием данного маршрутизатора выполняется мероприятие по необходимой модернизации технической защиты информационной системы предприятия на уровне распределения информации.

В АО «Нител» распределение информационных потоков осуществляется на уровне предприятия - информация распределяется между подразделениями и службами предприятия и на уровне структурного подразделения - до уровня конкретного автоматизированного рабочего места.

На уровне ядра обеспечивается высокоскоростная передача трафика в самой сети, подключение к сети Интернет и т.д.

Серверная ферма представляет собой группу коммутаторов, формирующих подключение серверов к корпоративной сети, и обеспечивает ее высокую производительность и надежность.

Многоуровневая система уменьшает время простоя сети, минимизирует потери рабочего времени, организует индивидуальный подход к выполнению требований пользователей, внедрение дополнительных приложений и сервисов.

3.3 Анализ информации, существующей на предприятии. Организация работы с информацией для служебного пользования

Единая политика безопасности, функционирующая на предприятии, включает в себя общие принципы защиты информации, правила классификации информации по степени важности, систему организации и разграничения доступов к информации, требования к работе с информацией и нормы ответственности за несоблюдение правил безопасности [9].

Информация, существующая на предприятии, делится на следующие основные виды: общедоступную и ограниченного доступа, которую можно разделить на информацию служебного пользования (ДСП), конфиденциальную и секретную.

Общедоступная информация – это информация, которая не составляет какую-либо тайну и доступна сотрудникам в локальной сети предприятия со

своих автоматизированных рабочих мест. Общий портал предприятия – это корпоративная информационная сеть, в которой размещены информация о текущих общих приказах генерального директора, сайты отделов, телефонные справочники, корпоративная почта, технические библиотеки, библиотеки конструкторских, технологических документов и др. Доступ к этой информации имеют все сотрудники со своих автоматизированных рабочих мест в режиме чтения.

Секретные документы в печатном виде хранятся в помещении с режимным доступом, снабженном видеокамерами, бесконтрольное проникновение в них полностью исключено. Данные документы существуют на предприятии только в бумажном виде.

К конфиденциальной информации относятся персональные данные сотрудников предприятия, коммерческая тайна. Данные документы могут быть как в бумажном, так и в электронном виде. В электронном виде эта информация хранится на специально выделенном для этого сервере, доступ к которому возможен только сотрудникам, непосредственно работающими с этими данными в силу своей профессиональной деятельности.

К документам служебного пользования «относится несекретная информация, касающаяся деятельности организации, ограничения на распространение которой диктуются служебной необходимостью. Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений» [21, п.1.2].

Актуальность присвоения литеры ДСП документам на предприятии определяет руководитель проекта или структурного подразделения. Литера ДСП на документах определяет следующие ограничения:

– запрет на ознакомление с ней лиц, не имеющих доступ к данной информации,
– запрет на копирование. Документы с данной литерой не подлежат копированию и сохранению копий.

Сейчас конструкторская и технологическая служебная документация разрабатывается в электронном виде, затем распечатывается на плоттере, после чего ей присваивается литера ДСП, ставится штамп «Для служебного пользования» и в этом виде хранится в выделенных режимных помещениях, доступ к которым ограничен и возможен только при служебной необходимости. И это очень неудобно для оперативного решения производственных вопросов, т.к. приходится тратить время на поиски необходимой информации в специализированных архивах, а принимать решения приходится быстро.

В настоящее время на предприятии существует острая необходимость разработки и хранения документов для служебного пользования в электронном виде и формировании к ним доступа ведущих специалистов, в чьи обязанности входит работа с этими данными.

Перед организацией такой работы необходимо понимать, что электронный документ – это документ, который создан и подписан в электронном виде. Он не является бумажным документом, который отсканировали после всех процедур согласования. Использование и хранение электронных документов должно быть оговорено во внутреннем регламенте предприятия. Этот документ необходимо определенным способом обработать, чтобы обеспечить его защиту и сохранность, и зафиксировать передачу в архив.

Организация работы с электронными документами с литерой ДСП требует особого внимания, т.к. эти документы должны учитываться отдельно от общедоступных, работать с ними можно только на аттестованных по требованиям защиты информации компьютерах.

Первое решение этой задачи, наиболее простое для обеспечения информационной безопасности, - сформировать отдельную сеть, состоящую из нескольких, не подключенных к общей корпоративной сети, компьютеров в режимном помещении с организацией видеонаблюдения и системы СКУД, с соответствующими правами доступа сотрудников к этой служебной информации. Это будет изолированная система со своими документами, настройками, справочниками и т.д. Выстраивание этой системы начинается с

нуля, что позволит четко спланировать ее защиту и аттестовать, не затрагивая основную сеть. Но в этом случае сотруднику предприятия необходимо работать в режимном помещении, т.е. отсутствовать на своем основном рабочем месте. Доступ к документам с литерой ДСП имеют руководители и ведущие специалисты многих подразделений, территориально расположенных в различных зданиях, и отсутствие их на рабочем месте не всегда удобно для решения текущих и срочных вопросов.

Но есть и другой метод организации работы, который заключается в том, чтобы определенному количеству пользователей организовать во внутренней сети предприятия необходимый защищенный доступ как документам общего пользования, так и к документам ДСП.

И этот подход наиболее удобен для организации работы ведущих специалистов предприятия. Работникам не надо менять рабочие места и интерфейс системы. Документы общего пользования и документы ДСП могут поступают на рабочие места по соответствующему регламенту. Но этот подход ведет к увеличению стоимости и времени работы, возникновению определенных сложностей, анализу информационной защиты системы и т.д.

Общая схема подключения показана на рисунке 6, где АРМ1 – автоматизированное рабочее место для работы с общедоступной информацией; АРМ2 – автоматизированное рабочее место для работы как с общедоступной информацией, так и служебной.

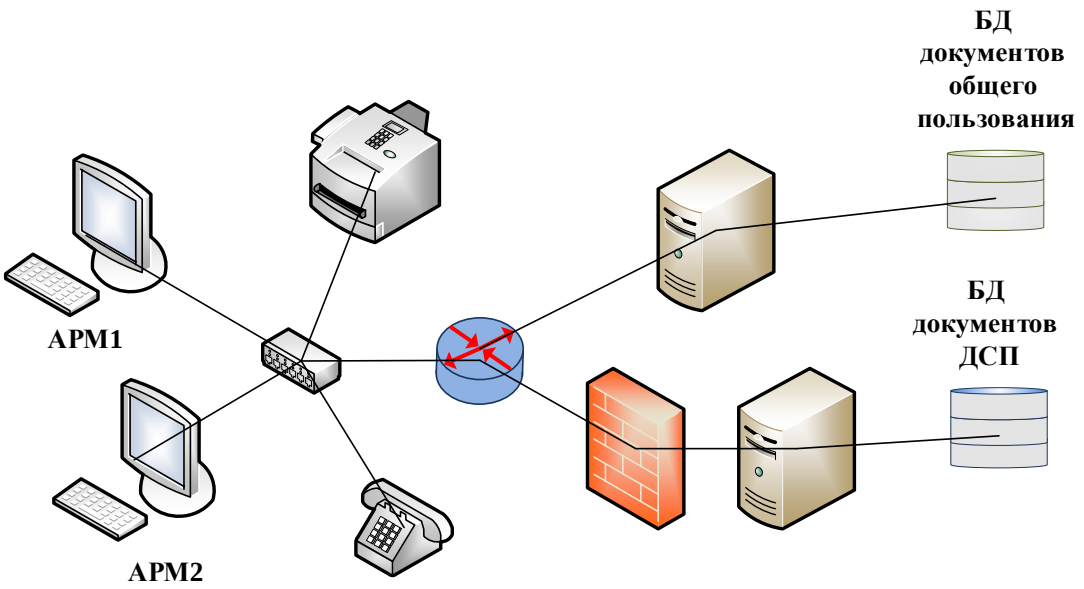


Рисунок 6 – Организация доступа к документам общего пользования и документам ДСП

Документы общего пользования и документы ДСП поступают на рабочие места по соответствующему регламенту. Но этот подход предполагает организацию многофакторного доступа к служебной информации, что пока не реализовано на предприятии. Сейчас доступ к автоматизированному рабочему месту для всех сотрудников осуществляется с помощью однофакторной аутентификации – логина и пароля. Для доступа к служебной информации для привилегированных пользователей существует дополнительная аутентификация с расширенным логином [10]. Но этот доступ не является многофакторным, и, как временное решение, вполне допустим во внутренней сети предприятия при соблюдении всех рабочих инструкций по информационной безопасности.

Для организации защиты информации ДСП в локальной сети предприятия необходимо решить две основные группы задачи.

Первая группа задач состоит в своевременном и достаточном обеспечении необходимой открытой и ДСП информацией сотрудников предприятия, имеющих к ней доступ, для реализации своих профессиональных функций. В данном случае организация работы с общедоступной информацией ничем не

ограничивается, кроме ее фактического наличия. А для работы с документами ДСП существует ограничение – необходим соответствующий допуск к служебной информации. Следовательно, при организации доступа сотрудника к закрытой информации имеется некоторое противоречие – во-первых, максимально ограничить его доступ к данной информации для уменьшения вероятности ее утечки и, во-вторых, предоставить необходимый доступный объем информации для решения служебных задач.

Для решения второй группы задач необходимо обеспечить предотвращение утраты информации, ее несанкционированного уничтожения информации и модификации, невмешательство в информационные системы, сохранение секретности информации в соответствии с правилами ее защиты и т.д.

Для корректной и безошибочной организации доступа к документам ДСП руководители подразделений должны четко обосновать необходимость работы своих сотрудников с данными документами и установить структуру и объемы этих работ [7].

До внедрения системы электронного доступа к документам ДСП надо определить и оценить угрозы защиты информации на предприятии, ведущие к ее изменению, блокированию, уничтожению или несанкционированному копированию [1]. Такими угрозами являются противоправные и ошибочные действия как самих работников предприятия, так и третьих лиц, а также отказы и сбой технических средств. Сотрудники, в результате нарушения правил информационной безопасности, могут похитить финансовые документы, информацию по клиентской базе, различные отчеты по проводимым научным и производственным проектам и т.д. И эти нарушения могут быть не обязательно умышленными. Просто забыли документы на принтере, неправильно уничтожили черновые варианты проектов, немного похвастались новыми разработками перед друзьями и т.д. Как видно, наиболее уязвимой точкой в системе защиты информации является человеческий фактор. Угрозы со стороны

работников предприятия наносят немалый ущерб, потому что реализуются без больших финансовых затрат и достаточно легко.

Организация разработки электронных документов ДСП и работа с ними в информационной сети предприятия требует соблюдения необходимых мер информационной безопасности. В настоящее время безопасность этой информации гарантируется исключительно сознательным поведением сотрудников. Для исключения возможных инцидентов необходимо разработать матрицу доступа к документам ДСП, рассмотреть и выбрать методы многофакторной аутентификации при организации работы с ними.

Вся информация, циркулирующая на предприятия, вне зависимости от степени секретности нуждается в защите от несанкционированного доступа, модификации и изменения информации [22]. Доступ к этим данным необходимо организовать в зависимости от уровня доступа сотрудников и их профессиональных занятий.

3.4 Анализ существующих моделей доступа и выбор модели матрицы доступа к служебной информации

3.4.1 Модель разграничения доступа на основе дискретной политики

В ГОСТе Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» [3] и в документах Гостехкомиссии РФ определены дискретное и мандатное управления доступом.

Дискретное разграничение доступом формирует доступ между однозначно определенными субъектами и объектами. Данная модель представляет собой дискретный набор «субъект (пользователь) – поток (операция) - объект». На практике данные модели основаны на прямоугольной матрице доступа, строками которой являются субъекты доступа, а столбцами – объекты. В ячейках на пересечении строк и столбцов записываются разрешенные действия субъектов над объектами, например, читать «r»,

копировать «c», писать «w», выполнять «e», печатать «pr» и др. [2]. Пример данной матрицы показан в таблице 2.

Таблица 2 – Матрица дискретного разграничения доступа

Субъект	Объект				
	O_1	O_2	…	O_{j-1}	O_j
S_1	crw	rw	…	rw	pr
S_2	c	rw	…	rw	pr
…	…	…	…	…	…
S_{i-1}	r	re	…	re	pr
S_i	r	re	…	re	pr

При дискретном разграничении для любой возможной комбинации «субъект (пользователь) – объект» доступ к информации однозначно разрешается или запрещается. В данном случае организация доступа происходит тщательным образом – до уровня отдельно взятого субъекта, отдельно взятого объекта доступа и отдельно взятой операции.

Недостатком данной модели является то, что субъект, имеющий доступ к чтению какой-либо конфиденциальной информации может передать ее другому, не имеющего доступа к ней.

3.4.2 Модель разграничения доступа на основе мандатной политики

Политика мандатного доступа основана на разграничении доступа субъектов к объектам на основе уровня доступа субъекта и защитной метки объекта, т.е. это способ разграничения доступа с фиксированным набором полномочий. Для всех субъектов определяют уровень доступа, а для объекта – уровень конфиденциальности, так называемый мандатный уровень или мандатная метка. Метка конфиденциальности субъекту присваивается при входе в сеть, а метку конфиденциальности объекту (файлу, каталогу)

присваивает субъект при его создании. Метки конфиденциальности субъекта и созданного им объекта равны.

При мандатной организации доступа разграничение осуществляется до уровня группы пользователей с определенным уровнем допуска и группы объектов с определенным уровнем конфиденциальности. Данный метод разграничения доступа показан на рисунке 7.

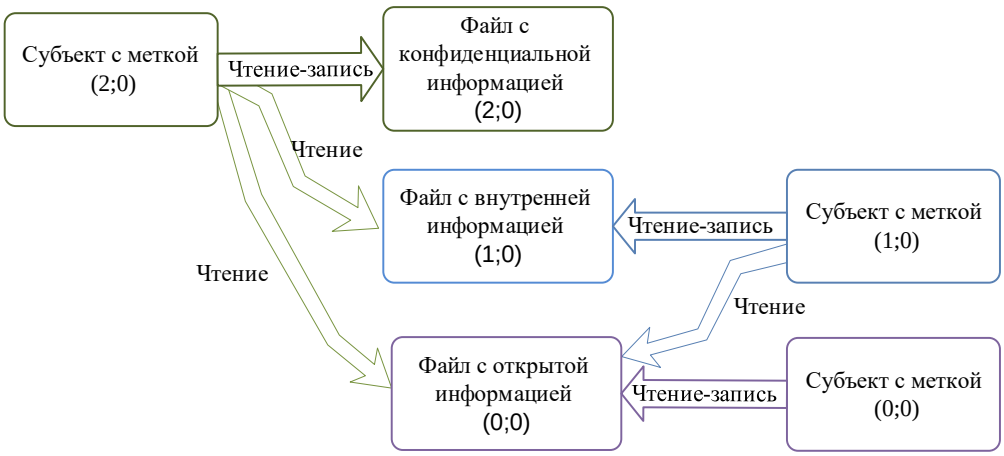


Рисунок 7 – Мандатное разграничение доступа к данным

В рамках этой модели нельзя превышать назначенный уровень доступа. Субъекты не могут наделять правами доступа другие субъекты, такими полномочиями обладают администратор сети или сотрудник отдела безопасности.

3.4.3 Модели разграничения доступа на основе тематической и ролевой политик

Базовые политики разграничения доступа – дискреционная и мандатная отражают не все организационно-технологические схемы защиты информации. На их основе разработаны тематическая и ролевая политики доступа.

При тематической политике субъекты объединяют в группы пользователей, работающих с информацией определенной тематики, а объекты

– в набор данных по аналогичной направленности. Субъекты наделяются полномочиями для создания и изменения информации в разрешенных тематических объектах.

На практике это выглядит следующим образом. На предприятии все документы в базах данных разделены по конкретным темам, т.е. у них существует некая метка классификатора. Сотрудники предприятия в соответствии со своими функциональными обязанностями получают права для работы с документами определенной тематики.

В модели на основе ролевой политики доступ формируется путем введения дополнительных абстрактных сущностей – ролей, соответствующих идентичным субъектам доступа, под которыми выступают конкретные пользователи с доступом, присущим этой роли.

При организации доступа на предприятии на основе ролевой политики сотрудники предприятия выполняют определенные функциональные обязанности в рамках некоторой должности, т. е. роли, с которой он и получает некоторый определенный набор прав и полномочий.

Количество ролей в системе может не соответствовать количеству пользователей, т.к. сотрудник предприятия, выполняющий много обязанностей и имеющий различные полномочия, может иметь несколько ролей, а сотрудникам, выполняющим одинаковую работу, назначается в системе одна роль.

Ролевая политика доступа наиболее распространена в организациях, т.к. сотрудники работают не от своего имени, а выполняют определенные служебные обязанности.

Для организации ролевого разграничения доступа сначала необходимо создать роли, определить их полномочия и затем назначить роли пользователям системы. Следовательно, при доступе в систему пользователь сначала авторизуется с присущей ему ролью, а их может быть несколько, а затем получает разрешение или запрет на пользование объектами в соответствии с полномочиями ролей, с которыми он авторизован.

Управление доступом при ролевой политике делится на две части. В первой части осуществляется авторизация пользователя с одной или несколькими присущими ему ролями, а во второй – разрешение или запрет субъектам пользователя к объектам системы в соответствии с полномочиями ролей, с которыми авторизован пользователь.

Для ролевых моделей характерен мандатный подход, при котором существуют строгие правила разграничения доступа через определенное группирование субъектов и объектов доступа, и дискреционный подход, определяющий гибкое разграничение доступа на конкретные функционально-организационные процессы.

3.5 Разработка модели формирования защищенного доступа к служебной информации

Основной задачей по защите информации является организация доступа к информационным ресурсам, базам данных, содержащим служебные сведения. Важно четко и однозначно определить кого, когда и к каким документам необходимо допускать.

По результатам исследования уровня информационной безопасности в 2023 г в организациях России было выявлено, что основными виновниками утечек данных являются топ-менеджеры – 8%, руководители направлений - 12%, линейные руководители -71%, линейные сотрудники - 71%, контрагенты – 14% и внештатные специалисты – 13%. В лидерах нарушений всегда держатся утечки данных (66 %), т.к. эти инциденты можно выявить с помощью средств защиты [33].

«В отличие от угроз информационной безопасности, реализуемых внешним злоумышленником, угрозы, исходящие от сотрудников организации, менее прогнозируемы» [4]. Работа с электронными документами на предприятии будет осуществляться во внутренней сети, поэтому целесообразно использовать модель внутреннего нарушителя информационной безопасности.

Основными мерами защиты от угроз внутреннего нарушителя информационной безопасности являются:

- введение разграничительной системы доступа к информационным ресурсам и носителям информации;
- введение ограничений на подключение внешних носителей;
- антивирусная защита автоматизированных рабочих мест;
- контроль целостности программного обеспечения автоматизированных рабочих мест и наличия несанкционированных программ;
- контроль выполнения должностных функций;
- использование криптографических средств аутентификации пользователей и ресурсов;
- регистрация действий пользователей в системных журналах;
- регулярная смена паролей и ключей;
- резервное копирование данных и т.д.

«Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом автоматизированных систем. С другой стороны, они же являются основной движущей причиной и движущей силой нарушений и преступлений» [5].

Основным направлением работы предприятия является разработка и производство радиолокационных станций различного назначения. И большая часть конструкторской документации имеет шифр ДСП, доступ к которой необходим разработчикам и конструкторам этой техники для ведения изделий в производстве, осуществления ремонта, модернизации и внедрение новых разработок.

Постоянный доступ к документам ДСП на предприятии имеют руководители конструкторских и технологических подразделений, сопровождающих производство. Временный допуск к служебной информации необходим руководителям проектов, связанных с модернизацией оборудования

и внедрением новых изделий. Руководителями проектов, в основном, являются ведущие специалисты предприятия.

Решение о доступе к информации, отнесенной к служебной тайне, регламентирует генеральный директор предприятия, порядок доступа определяет руководитель подразделения или проекта в письменном виде - приказе. Данный приказ должен содержать схему должностного или именного доступа к информации – матрицу полномочий к информации и вид документа или часть его, к которому может быть допущен сотрудник.

Для организации работы с информацией ДСП в информационной системе необходимо разработать матрицу доступа. Основой данной матрицы будет выступать ролевая модель. Основные роли – это руководители подразделений и ведущие специалисты. Данную матрицу необходимо дополнить дискретным доступом руководителей проектов и сотрудников, занятых в конкретном проекте.

В данной матрице представлены отделы, связанные непосредственно с производством, его организацией и модернизацией изделий (таблица 3).

В таблице используются следующие обозначения:

- cr – создание,
- d – удаление,
- r – чтение,
- w – запись,
- e – выполнение,
- pr – печать,
- c – копирование,
- s – сканирование.

Таблица 3 – Матрица разграничения доступа

<table>
<tr><td rowspan="4">Субъект</td><td colspan="7">Объекты</td></tr>
<tr><td colspan="3">общедоступный документ</td><td colspan="4">документ с литерой ДСП</td></tr>
<tr><td rowspan="2">конструкторские документы</td><td rowspan="2">технологические документы</td><td rowspan="2">принтер, сканер</td><td rowspan="2">участники проекта</td><td colspan="2">конструкторские документы</td><td colspan="2">технологические документы</td></tr>
<tr><td>проект 1</td><td>проект 2</td><td>проект 1</td><td>проект 2</td></tr>
<tr><td>Начальник конструкторского отдела 1</td><td>cr, r</td><td>r</td><td>pr, c, s</td><td></td><td colspan="2">r, e</td><td colspan="2">r</td></tr>
<tr><td>Начальник конструкторского отдела 2</td><td>cr, r</td><td>r</td><td></td><td></td><td colspan="2">r, e</td><td colspan="2">r</td></tr>
<tr><td>Начальник технологического отдела</td><td>r</td><td>cr, r</td><td></td><td></td><td colspan="2">r</td><td colspan="2">r, e</td></tr>
<tr><td>Начальник коммерческого отдела</td><td>r, e</td><td>r, e</td><td></td><td></td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td>Главный экономист</td><td>r, e</td><td>r, e</td><td></td><td></td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td>Начальник информационного отдела</td><td>r, e</td><td>-</td><td></td><td></td><td colspan="2">r, e</td><td colspan="2">-</td></tr>
<tr><td>Начальник производственного отдела</td><td>r, e</td><td>r, e</td><td></td><td></td><td>r, e</td><td>r, e</td><td>r, e</td><td>r, e</td></tr>
<tr><td rowspan="3">Ведущий инженер-электроник</td><td rowspan="3">cr, r, w, e, d</td><td rowspan="3">-</td><td></td><td>ФИО</td><td>cr, r, w, e, d</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td></td><td>ФИО</td><td>-</td><td>cr, r, w, e, d</td><td>-</td><td>-</td></tr>
<tr><td></td><td>ФИО</td><td>r, e</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="3">Ведущий инженер-конструктор</td><td rowspan="3">cr, r, w, e, d</td><td rowspan="3">r</td><td></td><td>ФИО</td><td>cr, r, w, e, d</td><td>-</td><td>r</td><td></td></tr>
<tr><td></td><td>ФИО</td><td>r, e</td><td>r</td><td>r</td><td>r</td></tr>
<tr><td></td><td>ФИО</td><td>-</td><td>cr, r, w, e, d</td><td>r</td><td>-</td></tr>
</table>

Продолжение таблицы 3

<table>
<tr><td rowspan="4">Субъект</td><td colspan="7">Объекты</td></tr>
<tr><td colspan="3">общедоступный документ</td><td colspan="4">документ с литерой ДСП</td></tr>
<tr><td rowspan="2">конструкторские документы</td><td rowspan="2">технологические документы</td><td rowspan="2">принтер, сканер</td><td rowspan="2">участники проекта</td><td colspan="2">конструкторские документы</td><td colspan="2">технологические документы</td></tr>
<tr><td>проект 1</td><td>проект 2</td><td>проект 1</td><td>проект 2</td></tr>
<tr><td rowspan="3">Ведущий инженер-технолог</td><td rowspan="3">r</td><td rowspan="3">cr, r, w, e, d</td><td rowspan="12">pr, c, s</td><td>ФИО</td><td>-</td><td>-</td><td>cr, r, w, e, d</td><td>-</td></tr>
<tr><td>ФИО</td><td>-</td><td>r</td><td>-</td><td>cr, r, w, e, d</td></tr>
<tr><td>ФИО</td><td>-</td><td>-</td><td>r, e</td><td>-</td></tr>
<tr><td rowspan="3">Ведущий специалист коммерческого отдела</td><td rowspan="3">r, e</td><td rowspan="3">r, e</td><td>ФИО</td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td>ФИО</td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td>ФИО</td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td rowspan="2">Ведущий экономист</td><td rowspan="2">r, e</td><td rowspan="2">r, e</td><td>ФИО</td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td>ФИО</td><td colspan="2">r, e</td><td colspan="2">r, e</td></tr>
<tr><td rowspan="2">Ведущий инженер-программист</td><td rowspan="2">r, e</td><td rowspan="2">-</td><td>ФИО</td><td>r, e</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>ФИО</td><td>-</td><td>r, e</td><td>-</td><td>-</td></tr>
</table>

Для организации работы сотрудников предприятия с любой информацией в компьютерной сети предприятия необходимо провести аутентификацию пользователей. Технология аутентификации обеспечивает контроль доступа к системам, проверяя, совпадают ли учетные данные пользователя с учетными данными в базе данных авторизованных пользователей [36].

«Традиционная аутентификация, основанная лишь на вводе логина и пароля, остается уязвимой перед угрозами, такими как подбор паролей, фишинг или утечка учетных данных. Для повышения уровня безопасности настоятельно рекомендуется внедрение многофакторной аутентификации, которая добавляет дополнительные слои проверки личности пользователя» [30].

В многофакторной аутентификации для разрешения доступа к информационным ресурсам личность пользователя удостоверяется на основании нескольких независимых признаков, в основном используется двухфакторная

аутентификация – метод проверки подлинности, при котором используются два различных фактора для подтверждения личности [11].

Первым фактором при реализации двухфакторная аутентификации выступает проверка логина и пароля, в качестве второго фактора могу быть подтверждения по электронной почте и СМС-рассылки, подтверждение личности с помощью биометрии и физические ключи безопасности [9].

Рассмотрим возможности реализации второго фактора аутентификации на предприятии.

Для применения метода аутентификации с помощью СМС-рассылки и сообщения на электронную почту необходимо, чтобы сотрудник указал сотруднику безопасности свой номер телефона или свою личную электронную почту, на которую он может выйти с помощью телефона. Но доступ к телефонам на предприятии ограничен в некоторых подразделениях, также возможно и отсутствие связи на территории. Методы подтверждения по электронной почте и СМС-рассылки для предприятия категорически не подходят. Они обязывают иметь при себе телефон и постоянный доступ к электронной почте, но при работе на автоматизированных рабочих местах, не привязанных к информационной сети предприятия и нахождении в защищенном от внешних воздействий помещениях, такой доступ осуществить невозможно.

Использование биометрии для доступа в корпоративную сеть существенно повышает информационную защищенность предприятия. Основными видами биометрических систем являются сканеры отпечатков пальцев, технологии распознавания лиц и др. [10]

Аутентификация по отпечатку пальцев считается самой доступной и быстрой в развертывании, такие сканеры подключаются к автоматизированному рабочему месту по интерфейсу USB. Это устройство поддерживает MS Windows и Linux OS. Например, цена одного настольного биометрического оптического сканера отпечатков пальцев FS80 компании BIOSMART – 12950 руб., в расчете на оборудование двухфакторной аутентификации необходимых 200

автоматизированных рабочих мест необходимо потратить 2 950 000 руб., т.е. требуются немалые финансовые вложения.

Для организации биометрии по распознаванию лиц необходима покупка более дорогостоящего оборудования. На автоматизированных рабочих местах на предприятии отсутствуют встроенные WEB-камеры для возможности использования биометрической аутентификации по лицу. Приобретение таких компьютеров также затратно.

Биометрические системы наиболее удобны с точки зрения пользователя, но для организации биометрического доступа закупка и установка необходимого специального оборудования и соответствующего программного обеспечения экономически не обоснована. Также для обработки персональных данных необходимы законные основания. Далеко не все сотрудники предприятия согласны на использование своих биометрических данных в качестве аутентификации для доступа к служебной информации.

Оптимальным решением внедрения обязательной двухфакторной аутентификации для предприятия является аппаратный метод – использование ключей безопасности – USB-токенов. USB-токен содержит уникальные данные, делающие доступ к корпоративной сети более защищенным.

В данном случае безопасность доступа основывается не только на знании пароля, но и на владении специальным устройством. Пароль может быть украден, но без устройства аутентификации – USB-токена – злоумышленник не получит доступ к системе. С помощью данного ключа осуществляется не только доступ к служебной или конфиденциальной информации, но и проверяется аппаратная подсистема в части изменения или замены элементов автоматизированного рабочего места. При неудачной попытке доступ к информации будет заблокирован.

Аутентификация осуществляется в следующем порядке:

– пользователь запрашивает доступ при помощи логина и пароля;
– аутентификация определяет, что идентификационные данные пользователя верны, и проверяет его полномочия;

– USB-токен физически подключается к системе, генерирует уникальную последовательность символов, при помощи которых происходит авторизация и предоставляется доступ к информации;
– токен хранится в устройстве до тех пор, пока пользователь не выйдет из системы.

Существуют различные токены, они отличаются параметрами защиты, функционалом и сферой применения.

USB-токены – современные ключевые носители и средства криптографической защиты информации, используемые для двухфакторной аутентификации и электронной цифровой подписи (ЭЦП). ЭЦП представляет собой некоторую аутентифицирующую информацию, которая передается вместе с подписываемым материалом. Отправитель формирует цифровую подпись с помощью своего секретного ключа, а получатель проверяет подпись с помощью открытого ключа отправителя.

Существуют простая, усиленная неквалифицированная и усиленная квалифицированная ЭЦП.

Простая подпись создается при помощи кода или пароля. Эта подпись идентифицирует автора документа, но не гарантируют неизменность документа с момента подписания.

Усиленная неквалифицированная подпись, сформированная с помощью криптографических средств, равноценна документам с ручной подписью и, в отличие от простой, гарантирует неизменность хранимых в системе документов.

Квалифицированная электронная подпись – это разновидность усиленной, но она сертифицирована и может являться аналогом документа с печатью [2]. На предприятии она применяется для оформления внешних документов.

Продукты Рутокен сертифицированы ФСТЭК России, и поэтому их можно применять в качестве второго фактора аутентификации на предприятии. Стоимость одного USB-токена – 2800 руб. и их общая покупка – 560 000 руб.

Разработка документов в электронном виде требует их утверждения электронной цифровой подписью. Поэтому параллельное использование USB-

токена для двухфакторной аутентификации и визирования электронных документов является наиболее приемлемым вариантов для предприятия.

«Аппаратные устройства обеспечивают максимальную защиту благодаря ограниченному вектору атак. Аппаратные решения значительно меньше зависят от операционных систем на рабочих станциях» [30].

Использование аппаратных устройств значительно снижает финансовые затраты, но здесь большую роль играет дисциплинированность сотрудников при работе со своими USB-токенами, их ответственность, исполнение всех принципов политики информационной безопасности по защите любой информации. «В отличие от угроз данным в сетях или на локальных компьютерах, которые реализуются весьма разнообразными атаками, угрозы, связанные с флешками, характеризуются очень мощными общими признаками возможных атак: 1) физическое завладение устройством и 2) получение доступа к его памяти на каком-либо персональном компьютере» [30]. Правила использования, хранения и утилизации USB-токенов зафиксированы в Положении по работе с машинными носителями информации, действующем на предприятии с 2024 года, с которой ознакомлены под личную подпись все сотрудники предприятия. В этом документе также определены порядок действий при утрате или краже токена, а также обязанности и ответственность его пользователя.

От несанкционированного доступа к служебной информации третьим лицам не застрахована практически ни одна корпоративная система. И если это произошло – присутствуют множественные недоработки в рабочем процессе. Своевременное реагирование на инциденты информационной безопасности, предотвращение нежелательных сценариев - главное условие, от которого зависит уровень защиты информации на предприятии.

3.6 Разработка Регламента реагирования на инциденты информационной безопасности

«Типовые политики информационной безопасности … не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей… для любой организации, серьезно относящейся к информационной безопасности, важно применять структурный и плановый подход к:

− обнаружению, оповещению об инцидентах информационной безопасности и их оценке;

− реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после негативных воздействий;

− извлечению уроков из инцидентов информационной безопасности, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности» [18, Введение].

Создание эффективной стратегии реагирования на инциденты и обеспечения устойчивости системы защиты информации стало первостепенной задачей на предприятии. Необходимо сосредоточиться на предотвращении атак, а также на выявлении и смягчении их последствий, быстром восстановлении информационной системы после нарушений [14]. Это включает в себя регулярные проверки безопасности, обучение сотрудников и выверенные шаги при реагировании на произошедшее событие [31].

В информационной сети предприятия процессы управления инцидентами не имеют своей формализации и определенного структурного порядка. Обработка происходящих инцидентов осуществляется «интуитивно», без четкого и последовательного подхода, что негативно отражается на уровне защищенности информации на предприятии. В результате отсутствия задокументированного процесса управления инцидентами происходит

регулярное повторение одних и тех же инцидентов информационной безопасности, неэффективные реагирование на них и последующий анализ, плохая координация действий между структурными подразделениями предприятия и бесполезное использование бюджета в части приобретения защитных технических средств.

Регламент реагирования на инциденты — это комплекс последовательных мероприятий по обнаружению и прекращению информационных атак, а также по анализу их причин, оценке ущерба и устранению последствий киберпреступлений [27]. Данный порядок действий должен быть закреплен в процедурах основной политики информационной безопасности предприятия.

Этапы и порядок реагирования на инциденты показаны на рисунке 8.

На этапе подготовки необходимо рассмотреть риски проникновения и утечки данных в структурах информационной системы, выделить различные сценарии возможных атак и определить ответственных сотрудников, их права, обязанности и порядок действий в случае наступления нежелательного события.

На этапе обнаружения с помощью систем обеспечения информационной безопасности определяется принадлежность произошедшего события к инциденту или нет.

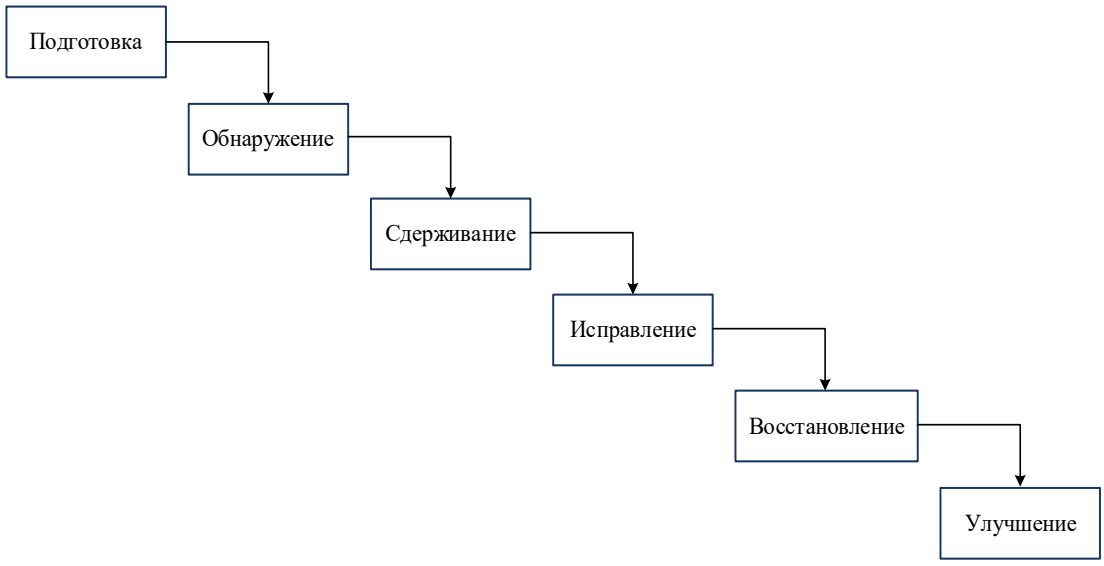


Рисунок 8 – Этапы и порядок реагирования на инциденты

Если событие считается инцидентом информационной безопасности, то предпринимаются дальнейшие шаги. При обнаружении реальной угрозы необходимо ее локализовать для ограничения воздействия и предотвращения дальнейшего ущерба, устранить уязвимость системы и выявить злоумышленника. Далее удалить части системы, использованные для передачи атаки, и восстановить затронутые системы, т.е. уничтожить вредоносные файлы и программы, сменить пароли пострадавших учетных записей, восстановить утраченные данные. На следующем этапе следует протестировать затронутые системы для обнаружения любых оставшихся угроз и предотвращения повторения аналогичных. После завершения восстановления необходимо провести анализ произошедшего инцидента, рассмотреть актуальность внесения изменений в программное обеспечение и оборудование, а также сформировать рекомендации для предотвращения подобных инцидентов.

Данный Регламент реагирования на инциденты информационной безопасности был разработан и внедрен в политику безопасности АО «Нител».

Регламент является необходимым для предприятия, т.к. позволит быстро идентифицировать любое событие или инцидент информационной безопасности и среагировать на него, повысить общую информационную безопасность за счет быстрого определения и реализации правильного решения, а также обеспечить средства предотвращения подобных инцидентов информационной безопасности в будущем [19].

Защита организации от угроз информационной безопасности является критически важным вопросом. Скорость реакции и корректность действия структурного подразделения, проводящего процедуры обнаружения, принятия решений, реагирования, проведения пост анализа и мероприятий по улучшению защитных мер, оказывает самое существенное влияние на величину ущерба от инцидентов информационной безопасности.

В третьей главе были разработаны и осуществлены мероприятия для повышения оценки текущего состояния информационной безопасности в АО «Нител» и усиления защиты информационной системы, для этого:

- изучена структура информационной системы предприятия и виды информации, функционирующие в данной системы. По результатам исследования определены правила организации работы с информацией ДСП в электронном виде;
- на основе ролевой политики доступа и модели внутреннего нарушителя информационной безопасности сформирована матрица разграничения доступа к служебной информации для сотрудников предприятия, одними из профессиональных обязанностей которых является разработка и модернизация продукции, выпускаемой предприятием. Но достаточно защищенный доступ к служебной и конфиденциальной информации будет обеспечен только при наличии двухфакторной аутентификации. В качестве второго фактора аутентификации был выбран USB-токен, имеющий сертификацию ФСТЭК и использование которого обосновано в качестве доступа к служебной и конфиденциальной информации и формированию ЭЦП;
- обоснована необходимость разработки на предприятии Регламента реагирования на инциденты информационной безопасности и рассмотрены основные этапы ее разработки.

Глава 4. Разработка и апробация модели оценки безопасности обновлений иностранного программного обеспечения. Оценка ее эффективности

4.1 Разработка и тестирование модели оценки безопасности обновлений зарубежного программного обеспечения

Безопасность и защита информации является первостепенной задачей для предприятия. Одним из самых важных аспектов обеспечения безопасности является регулярное обновление программного обеспечения, установленного в АО «Нител», основное из которых не является российской разработкой. Обновления программного обеспечения выпускаются с целью улучшения функциональности и исправления ошибок, они необходимы для поддержки новых функций, повышения безопасности, устранения уязвимостей или совместимости с новым оборудованием или операционными системами. Но обновления также могут нести и угрозу для стабильного функционирования информационной сети предприятия:

- содержать скрытые уязвимости, используемые для атак на инфраструктуру предприятия, в них может быть внедрен вирусный код для получения доступа к конфиденциальной информации на предприятии или нарушить бесперебойную работу его систем;
- обновления могут привести к проблемам совместимости с существующей ИТ-инфраструктурой;
- неконтролируемые обновления могут привести к убыткам из-за сбоя системы, утечек данных, кибератак, репутационным рискам т.д.

Поэтому перед установкой обновлений операционных систем иностранного производства необходимо провести исследование для оценки их влияния на функциональность, безопасность и производительность системы в рамках изолированной тестовой среды.

Целью данного исследования является разработка и апробация комплексной модели тестирования обновлений иностранного программного обеспечения в условиях изолированной среды. Такая модель позволит оценить степень безопасности обновленного программного обеспечения.

Алгоритм, представленный на рисунке 9 помогает принять решение об установке необходимого обновления.

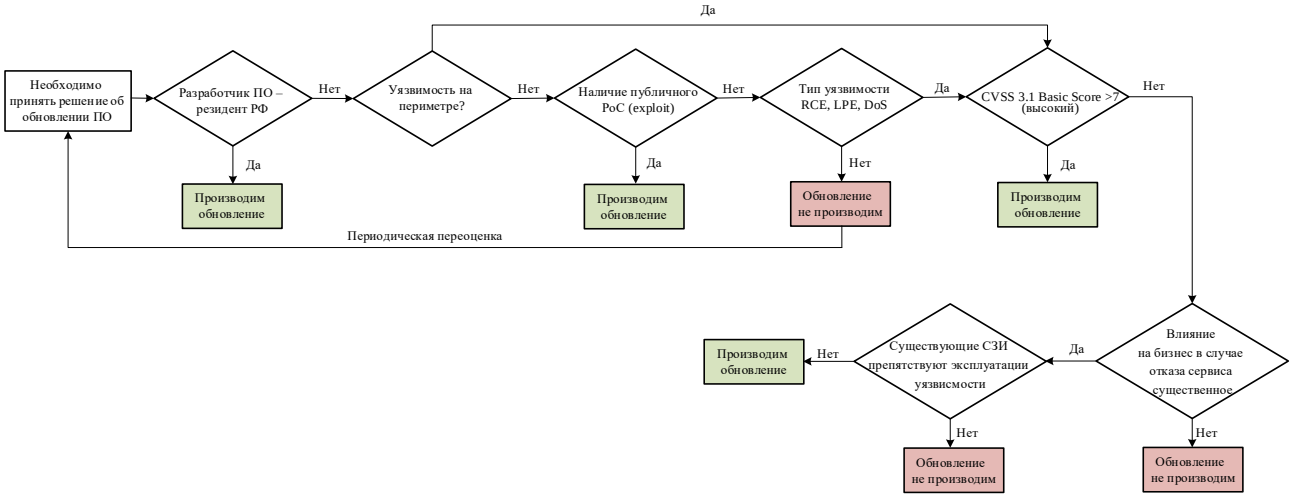


Рисунок 9 – Алгоритм принятия решения об установке обновления

Модель тестирования обновлений иностранного программного обеспечения показана на рисунке 10. Она представляет собой соединенные в изолированную тестовую сеть сервер и компьютеры. На сервере установлены приложения и сервисы (веб-серверы, БД), необходимые для функционирования предприятия, на компьютерах - разработанные тесты сценариев, имитирующие реальные действия пользователей и необходимые сетевые взаимодействия.

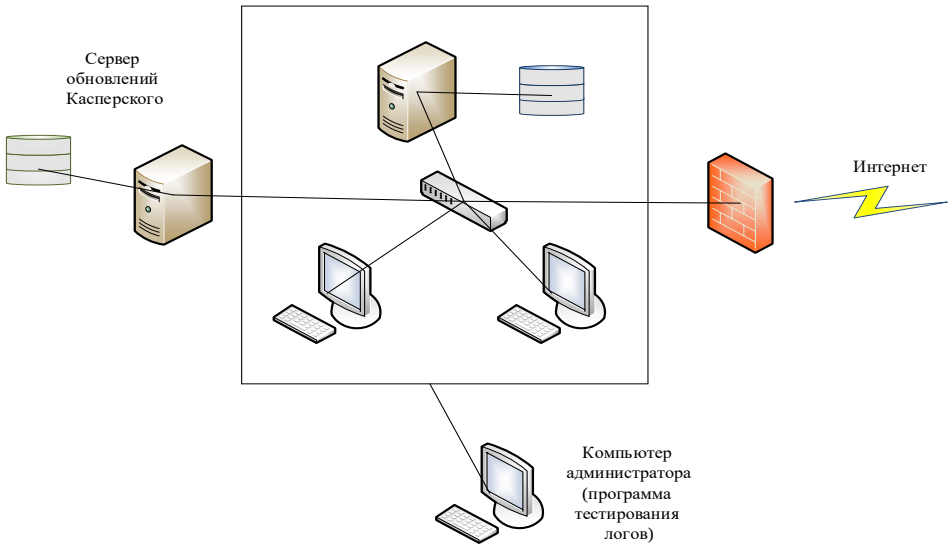


Рисунок 10 – Модель системы тестирования обновлений

До установки обновлений необходимо провести тестирование собранной системы, выполнить тесты имитации работы пользователя и сбор данных о производительности и сетевом трафике. Результаты данного теста приведены на рисунке 11.

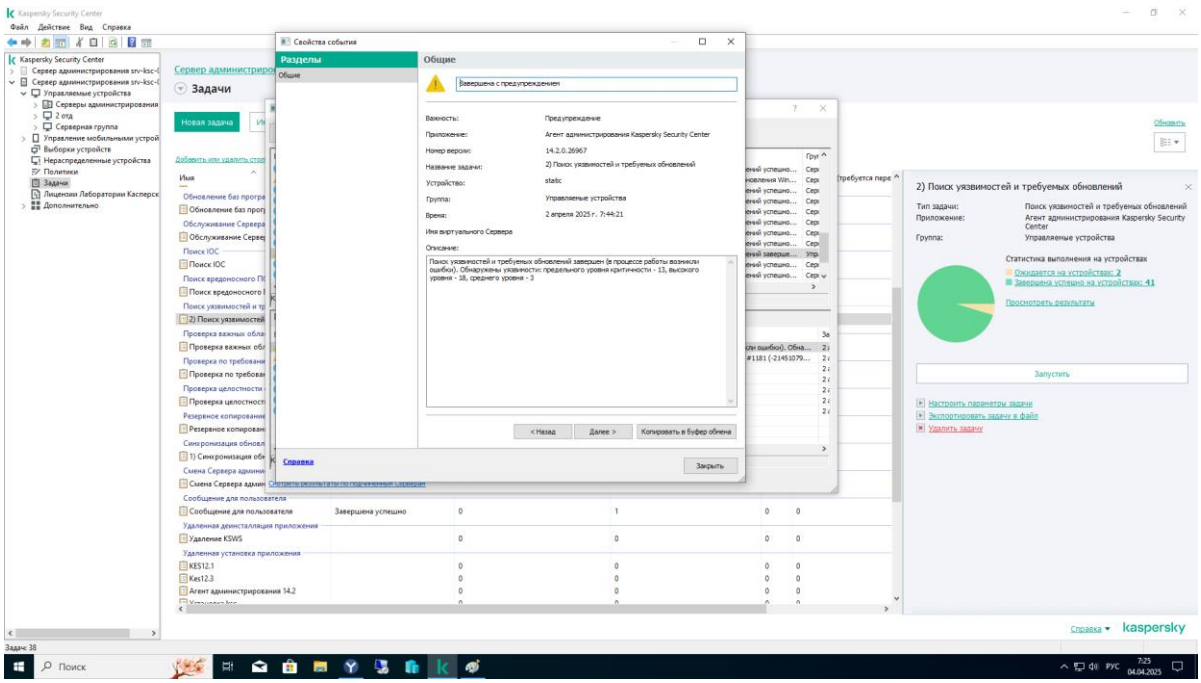


Рисунок 11 – Результаты теста до установки обновлений

Результатом теста является обнаружение 13 уязвимостей критического уровня, от которых необходимо избавиться на сервере Windows 2016.

Далее на сервер необходимо установить обновления для данной операционной системы, перезагрузить систему, чтобы убедиться, что все изменения ступили в силу.

На подключенных компьютерах запустить сценарии, имитирующие работу реальных пользователей. Эти тесты должны охватить наиболее важные операции и рабочие процессы критически важных функций системы, такие как, процессы входа в систему, работа с папками и файлами, запуск приложений, обмен данными через сеть и др., выполняемых пользователями в повседневной деятельности. Результаты тестирования системы после обновления системы показаны на рисунке 12.

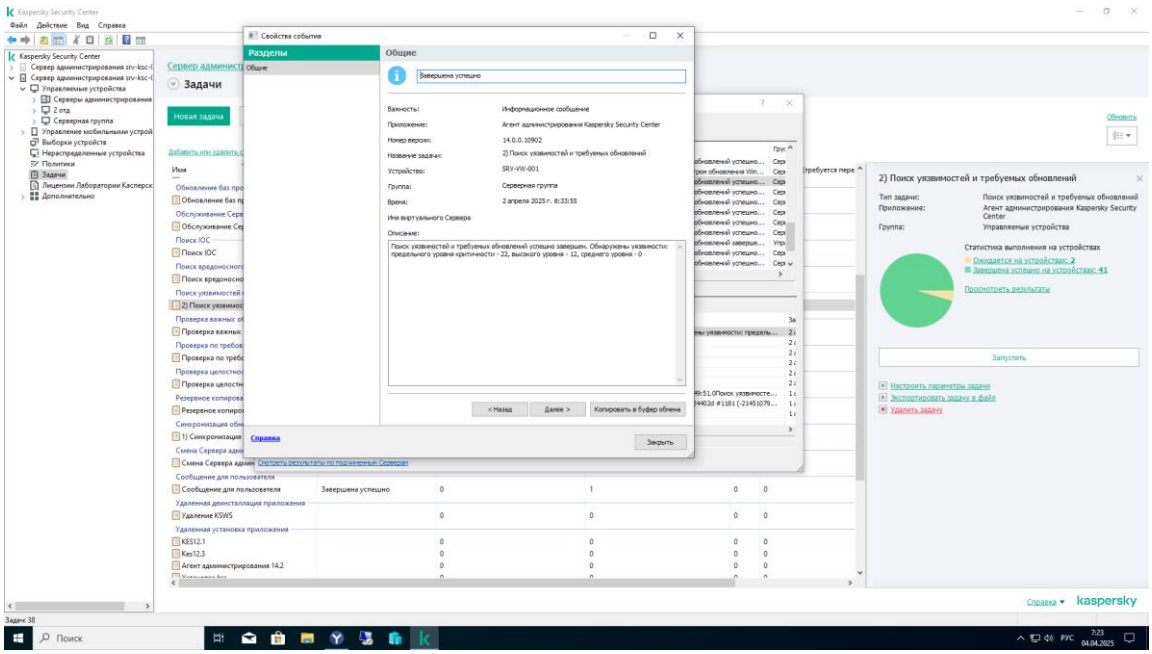


Рисунок 12 – Результаты теста после установки обновлений

Результатом теста является обнаружение 13 уязвимостей критического уровня, от которых необходимо избавиться на пользовательском компьютере с ОС Windows 10.

На рисунке 13 представлены обновления, которые необходимо установить после проведения тестирования операционной системы.

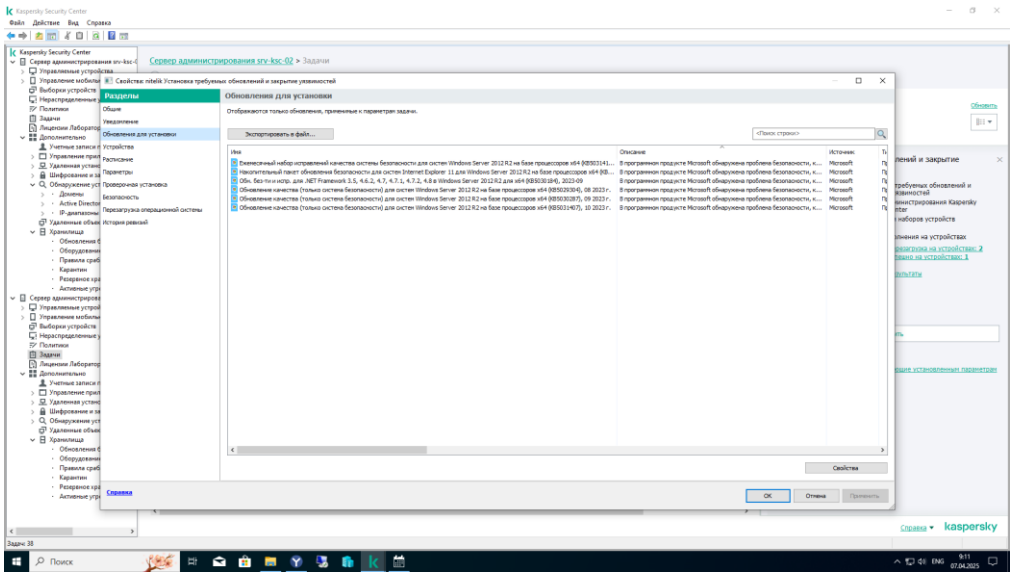


Рисунок 13 – Обновления, готовые для установки

Тесты, используемые в данном исследовании, их действие и ожидаемый результат, приведены в таблице 4.

Таблица 4 – Тесты, применяемые при исследовании модели

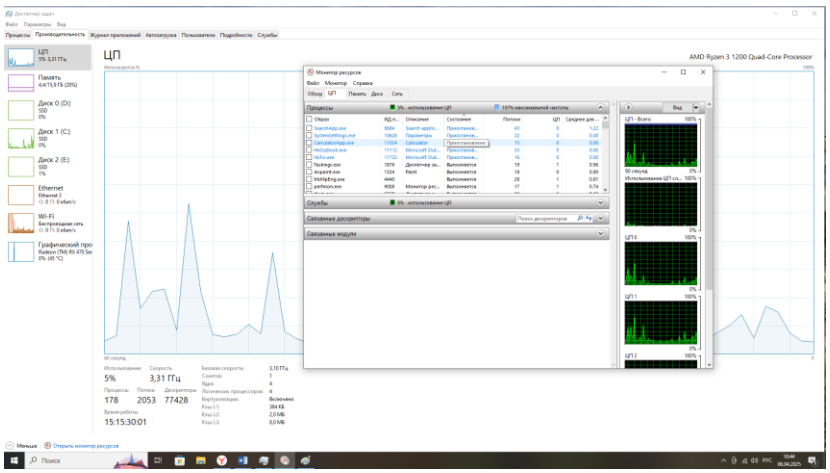
Тест	Действие	Ожидаемый результат
Вход в систему	пользователь вводит логин и пароль для доступа к серверу через SSH	успешная аутентификация и доступ к командной строке сервера
Работа с веб-сервером	пользователь открывает веб-сайт, размещенный на сервере, через браузер	веб-страница загружается без ошибок
Загрузка файлов	пользователь загружает файл на сервер через FTP	файл успешно загружен и доступен на сервере
Работа с базой данных	пользователь выполняет SQL-запросы к базе данных через клиент	запросы выполняются успешно, данные возвращаются корректно
Создание резервных копий	пользователь создает резервную копию данных на сервере	резервная копия успешно создана и доступна для восстановления

В процессе выполнения всех тестов необходимо настроить сбор логов на сервере и компьютерах с помощью инструментов мониторинга и анализа журнала ошибок для последующего исследования.

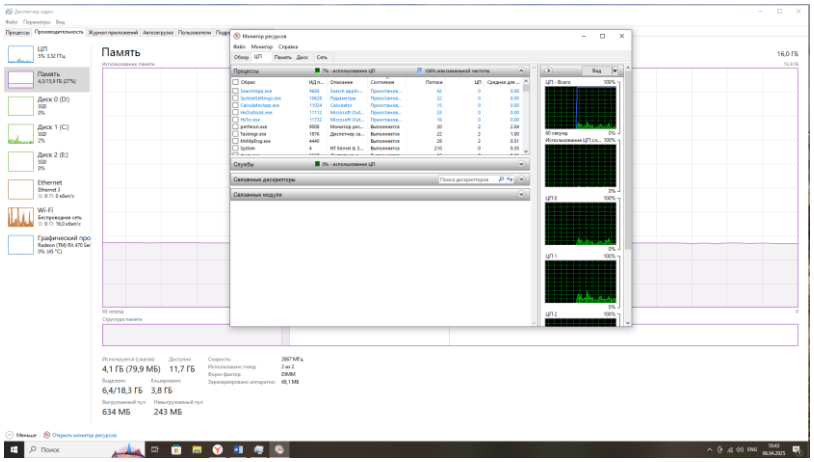
В процессе тестирования и по его окончании проводится анализ собранных данных на предмет ошибок, аномалий и сбоев.

Результаты исследования:

- производительность системы. Мониторинг нагрузки на ЦП и на память (рисунок 14) проводился в течение 5 дней. Вывод - нагрузка на данные модули осталась без изменений;
- сетевой трафик. Подозрительные соединения не обнаружены. Сетевой трафик соответствует ожидаемому поведению. Результат тестирования представлен на рисунке 15;
- функциональность сервисов. После обновления все системы (рисунок 16), сервисы (рисунок 17), включая веб-сервисы и базу данных, работают без сбоев;
- логи системы, которые необходимо обнаружить, показаны на рисунке 18;
- уязвимости. Сканирование системы не выявило критических уязвимостей. Отчеты о статистике уязвимостей и распределении уровней опасностей приведены на рисунке 19.

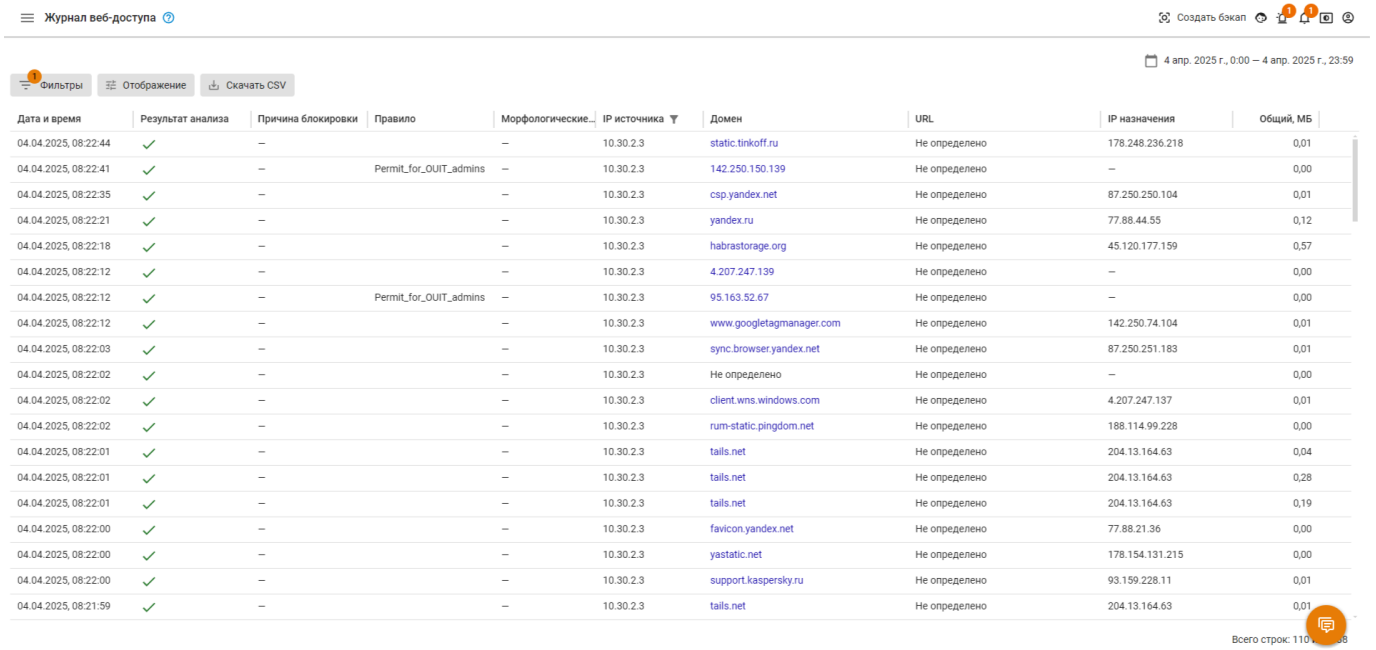


Мониторинг нагрузки на ЦП



Мониторинг нагрузки на память

Рисунок 14 – Скриншоты результатов мониторинга на ЦП и память



Дата и время	Результат анализа	Причина блокировки	Правило	Морфологические...	IP источника	Домен	URL	IP назначения	Общий, МБ
04.04.2025, 08:22:44	✓	–		–	10.30.2.3	static.tinkoff.ru	Не определено	178.248.236.218	0,01
04.04.2025, 08:22:41	✓	–	Permit_for_OUIT_admins	–	10.30.2.3	142.250.150.139	Не определено	–	0,00
04.04.2025, 08:22:35	✓	–		–	10.30.2.3	csp.yandex.net	Не определено	87.250.250.104	0,01
04.04.2025, 08:22:21	✓	–		–	10.30.2.3	yandex.ru	Не определено	77.88.44.55	0,12
04.04.2025, 08:22:18	✓	–		–	10.30.2.3	habrastorage.org	Не определено	45.120.177.159	0,57
04.04.2025, 08:22:12	✓	–		–	10.30.2.3	4.207.247.139	Не определено	–	0,00
04.04.2025, 08:22:12	✓	–	Permit_for_OUIT_admins	–	10.30.2.3	95.163.52.67	Не определено	–	0,00
04.04.2025, 08:22:12	✓	–		–	10.30.2.3	www.googletagmanager.com	Не определено	142.250.74.104	0,01
04.04.2025, 08:22:03	✓	–		–	10.30.2.3	sync.browser.yandex.net	Не определено	87.250.251.183	0,01
04.04.2025, 08:22:02	✓	–		–	10.30.2.3	Не определено	Не определено	–	0,00
04.04.2025, 08:22:02	✓	–		–	10.30.2.3	client.wns.windows.com	Не определено	4.207.247.137	0,01
04.04.2025, 08:22:02	✓	–		–	10.30.2.3	rum-static.pingdom.net	Не определено	188.114.99.228	0,00
04.04.2025, 08:22:01	✓	–		–	10.30.2.3	tails.net	Не определено	204.13.164.63	0,04
04.04.2025, 08:22:01	✓	–		–	10.30.2.3	tails.net	Не определено	204.13.164.63	0,28
04.04.2025, 08:22:01	✓	–		–	10.30.2.3	tails.net	Не определено	204.13.164.63	0,19
04.04.2025, 08:22:00	✓	–		–	10.30.2.3	favicon.yandex.net	Не определено	77.88.21.36	0,00
04.04.2025, 08:22:00	✓	–		–	10.30.2.3	yastatic.net	Не определено	178.154.131.215	0,00
04.04.2025, 08:22:00	✓	–		–	10.30.2.3	support.kaspersky.ru	Не определено	93.159.228.11	0,01
04.04.2025, 08:21:59	✓	–		–	10.30.2.3	tails.net	Не определено	204.13.164.63	0,01

Всего строк: 110

Рисунок 15 – Результаты тестирования СОВ и межсетевого экрана

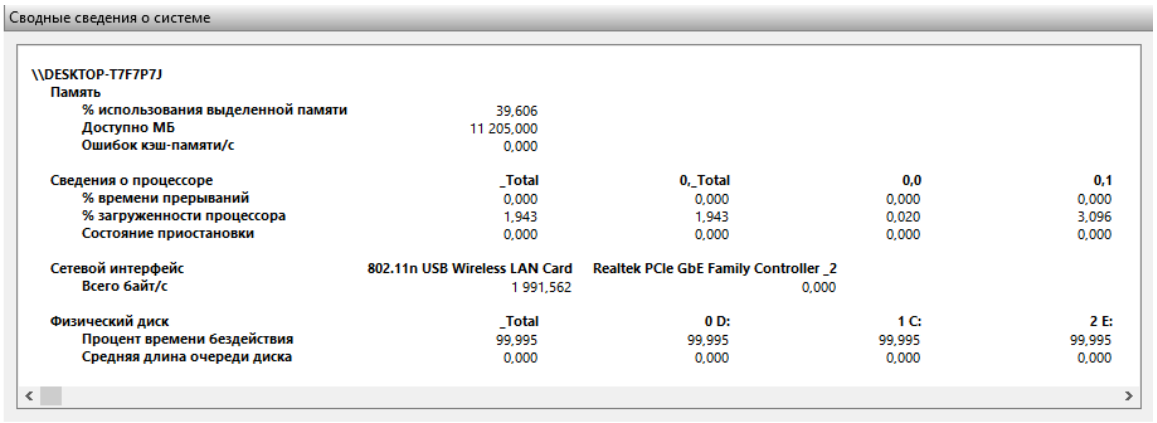


Рисунок 16 – Общие сведения о системе

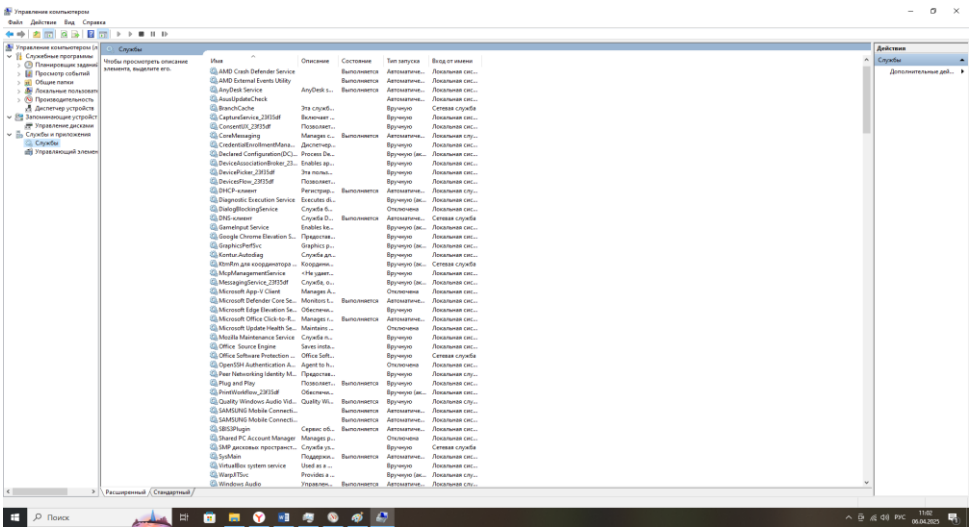


Рисунок 17 – Проверка серверов

Тип события	EventID
События входа и выхода	Successful logon 4624; failed logon 4625; logoff 4634, 4647 и т.д.
Изменение аккаунта	Created 4720; enabled 4726; changed 4738; disabled 4725; deleted 630
Изменение пароля	4724, 4723
Запуск и прекращение работы сервисов	7035,7036, и т.д.
Доступ к объектам	4656, 4663

Рисунок 18 – Найденные логи в системе

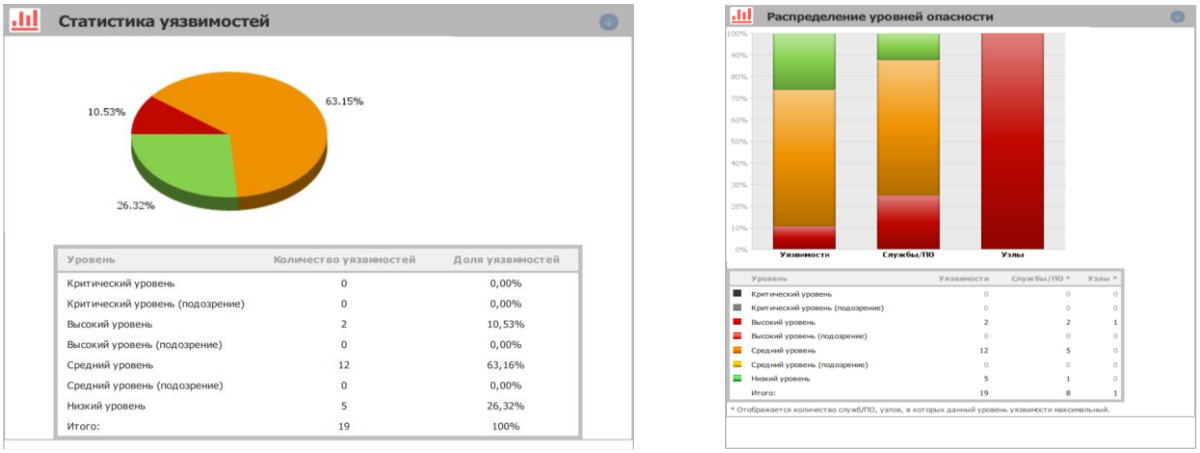


Рисунок 19 – Отчеты по тестированию уязвимостей

По результатам исследования определено, что установленное обновление показало положительные результаты:

- производительность не изменилась, нагрузка на систему не увеличилась, что косвенно свидетельствует об оптимизации обновлений при наличии других благоприятных результатов;
- отсутствие угроз. Подозрительные соединения не обнаружены, что подтверждает безопасность обновлений;
- функциональность сервисов. Все сервисы работают стабильно, что указывает на корректность внесенных изменений;
- снижение количества ошибок. Уменьшение ошибок в логах свидетельствует о повышении стабильности системы.

Проанализировав полученные результаты, можно сделать следующие выводы:

- тестирование обновления в тестовой системе позволяет безопасно оценить их влияние на систему,
- использование обновлений иностранного программного обеспечения в данном случае не выявило значительных рисков,
- результаты тестирования подтверждают возможность внедрения обновлений в производственную среду.

Данное исследование подтвердило эффективность тестирования обновлений серверных ОС. Положительные результаты тестирования демонстрируют безопасность и стабильность обновлений иностранного программного обеспечения. Результаты исследования могут быть использованы для улучшения процессов обеспечения информационной безопасности на предприятии.

Если при тестировании хотя бы на одном из компьютеров произойдет ошибка выполнения процесса обновления, после установки обновлений изменится статус постоянной защиты программы безопасности, будет найден зараженный объект или произойдет ошибка функционирования программы Kaspersky security center, то набор обновлений является вредоносным.

В процессе проведенного тестирования некорректного обновления выявлено не было.

Для непрерывного анализа обновления иностранного программного обеспечения лучше использовать автоматизированные тесты. Автоматизация тестовых действий пользователя – необходимый элемент для повышения эффективности и повторяемости процесса тестирования.

Некоторые методы и инструментов, используемые для автоматизации представлены на рисунке 20.

Автоматизация тестовых воздействий пользователя значительно упрощает процессы тестирования обновлений операционных систем. Преимуществами автоматизации являются:

- повышение скорости тестирования,
- уменьшение человеческих ошибок,
- возможность тестирования в любое время,
- легкость повторения тестов при изменении системы.

```
    Автоматизация входа в систему через SSH:
ssh user@server -i /path/to/private_key "command_to_execute"


    Автоматизация загрузки файлов через FTP:

        from ftplib import FTP
    ftp = FTP('server_address')
    ftp.login('user', 'password')
    ftp.storbinary('STOR filename.txt', open('localfile.txt', 'rb'))
    ftp.quit()


    Инструменты для автоматизации браузера
    from selenium import webdriver
driver = webdriver.Chrome()
driver.get("http://example.com")
driver.find_element("name", "username").send_keys("testuser")
driver.find_element("name", "password").send_keys("password123")
driver.find_element("name", "login").click()
driver.quit()

Инструменты для автоматизации работы с базами данных
from sqlalchemy import create_engine
engine = create_engine('postgresql://user:password@localhost/dbname')
with engine.connect() as connection:
    result = connection.execute("SELECT * FROM table_name")
    for row in result:
        print(row)

    Инструменты для автоматизации ввода с клавиатуры и мыши
            Send, Hello World{Enter}
    MouseMove, 100, 200
    Click

          Управление сценариями
           - name: Execute SSH command
           hosts: server
           tasks:
             - name: Run a command
               command: /path/to/script.sh

        Автоматизация загрузки веб-страницы:
                  from selenium import webdriver
        driver = webdriver.Chrome()
        driver.get("http://example.com")
        print("Page title:", driver.title)
        driver.quit()


    Автоматизация загрузки файла на сервер:
       from ftplib import FTP
    ftp = FTP('server_address')
    ftp.login('user', 'password')
    ftp.storbinary('STOR filename.txt', open('localfile.txt', 'rb'))
    ftp.quit()
```

Рисунок 20 – Скрипты и инструменты для автоматизации тестирования обновлений

4.2 Оценка эффективности разработанной модели

Оценка экономического эффекта затрат разработанного на предприятии программного решения (проектный вариант) проведена на сравнении затрат на разработку аналогичного модуля по договору внешним программистом (базовый вариант).

Затраты для расчета себестоимости проектного модуля тестирования «определяются составом привлекаемых для решения задачи специалистов-исполнителей» [15]. Данную разработку осуществили программист и сотрудник отдела безопасности предприятия.

Для расчета базового варианта модели необходимы следующие данные:

- предполагаемое время разработки – 80 часов;
- стоимость услуг наемного программиста необходимой квалификации за один час работы составляет от 2000 руб. [25].

Расчет себестоимости обоих вариантов представлен в таблице 5.

Таблица 5 – Расчет себестоимости разработки модели тестирования обновлений

Статьи расходов	Затраты, руб.	
	базовый вариант	проектный вариант
Зарплата исполнителей	2 000 · 80	38 000 + 42 000
Социальные страховые выплаты	0,271 · 2000 · 80	0,3·(38 000 + 42 000)
Прочие прямые расходы	0	0
Накладные расходы	0	0
Итого	203 360	104 000

В таблице 6 показан расчет показателей экономической эффективности разработки системы тестирования обновлений иностранного программного обеспечения базового и проектного вариантов, на рисунке 21 приведено сравнение затрат.

Таблица 6 – Расчет эффективности разработки модуля тестирования обновлений

Затраты (руб.)		Абсолютное изменение затрат ΔЗ=ЗБ-ЗП	Коэффициент относительного изменения затрат К= ΔЗ/ЗБ ·100%	Индекс снижения затрат Y= ЗБ/ЗП
базовый вариант (ЗБ)	проектный вариант (ЗП)			
203360	104000	99 360	48	1,9

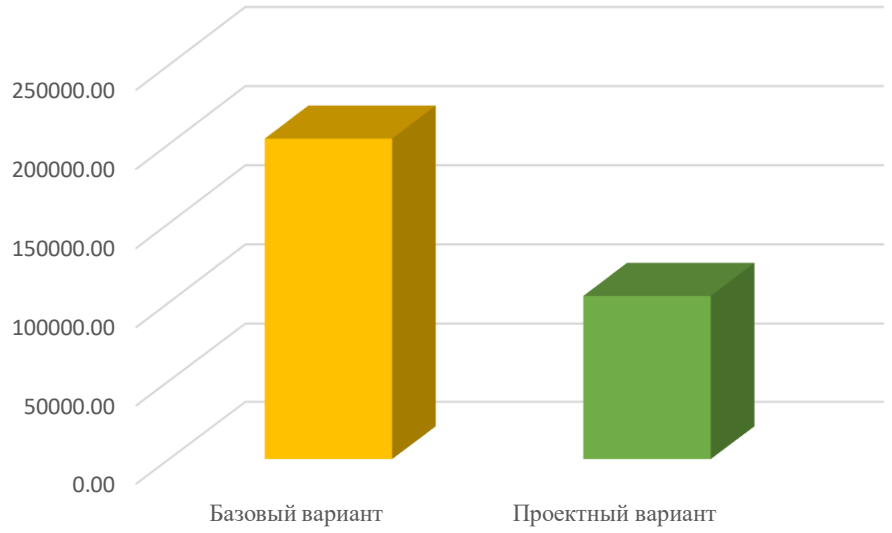


Рисунок 21 – Сравнение затрат на разработки модуля тестирования обновлений

Как следует из расчетов, затраты на разработку модуля специалистов предприятия меньше в 1,9 раз, чем при привлечении сторонних работников.

Срок окупаемости данного проекта рассчитаем по формуле (3):

$$Т = Зт / ΔЗ \text{ (мес.)}, \quad (3)$$

где Зт – затраты на реализацию разработанного решения.

$$Т = 104000 / 99360 \approx 1 \text{ мес.}$$

Данный расчет показал эффективность разработки модуля тестирования обновлений иностранного программного обеспечения силами сотрудников

предприятия, срок окупаемости средств, затраченных на данную разработку, составляет 1 месяц.

В данной главе разработана и исследована модель оценки влияния обновлений программного обеспечения иностранного производства, необходимость которой обусловлена вероятным наличием скрытых уязвимостей или вредоносного кода.

Тестирование обновлений иностранного программного обеспечения также позволит перенести переход на отечественные программные аналоги и применять уже проверенные решения, интегрированные в производственную инфраструктуру предприятия.

Глава 5 Апробация эффективности выполнения мероприятий для повышения показателя защищенности информационной безопасности

Для апробации результатов работ по повышению информационной безопасности предприятия необходимо определить эффективность комплекса осуществленных мероприятий по защите информации и провести повторную оценку показателя состояния технической защиты информации.

Экономическая оценка выполненной работы по модернизации информационной системы предприятия проведена на основе анализа целесообразности произведенных затрат для достижения минимального уровня защиты от типовых актуальных угроз безопасности информации

5.1 Определение экономических затрат на модернизацию системы безопасности

Проанализировав данные таблицы 1 и выполнив необходимые расчеты можно определить приблизительные финансовые потери предприятия при реализации некоторой информационной атаки – 2618 млн руб. Данная сумма очень существенна для предприятия.

Для повышения уровня защищенности информации на предприятии были запланированы и выполнены следующие мероприятия:

- введение должности ответственного за обеспечение информационной безопасности и определение его обязанностей;
- установка маршрутизаторов уровня L3/L4;
- введение средств двухфакторной аутентификации;
- разработка матрицы доступа к служебной информации;
- формировании контроля учетных записей работников и их исключение при прекращении договорных или трудовых отношений;

– разработка документа о порядке реагирования на компьютерные инциденты.

Для определения результативности осуществленных работ рассмотрим предполагаемые угрозы и реализованные меры их противодействия (таблица 7).

Таблица 7 – Угрозы и меры противодействия

Угрозы	Меры противодействия
Деятельность компьютерных вирусов и инсайдерских программ	коммутатор уровня L3/L4
	комплекс мер по реагированию на информационные угрозы
Злоумышленные или случайные действия сотрудников предприятия	средства аутентификации
	разделение доступа к информации
	усиление административной ответственности
Несанкционированные действия людей, не являющихся сотрудниками предприятия	средства аутентификации
	быстрое реагирование на отключение доступа к информационной сети предприятия уволенных сотрудников

В таблицах 8 и 9 представлены стоимость закупленного оборудования и затраты на разработку необходимой документации.

Таблица 8 – Стоимость закупленного оборудования

Оборудование	Стоимость за единицу, руб.	Количество	Общая стоимость, руб.
Маршрутизатор уровня L3/L4	82 760	20	1 655 200
Рутокен	2 800	200	560 000
Провода и прочие расходные материалы	68 000	1	68 000
Программное обеспечение	50 000	1	50 000
Итого			2 333 200

Таблица 9 – Затраты на разработку документации для защиты данных.

Общие организационные мероприятия	
Проводимые действия	Стоимость, руб.
Разработка и оформление приказа	25 000
Разработка Регламента реагирования на инциденты	180 000
Доведение информации до сотрудников	35 000
Мероприятия в части ПО	
Разработка матрицы доступа	145 000
Организация взаимодействия с отделом кадров	10 000
Итого	395 000

Стоимость работ по реализации организационных мероприятий составила 395 000 руб.

Итоговая совокупность затрат на выполнение мероприятий по повышению защиты информации в информационной системе предприятия равна 2 728 200 руб. На рисунке 22 показано сравнение суммы, потраченной на реализацию мероприятий, и суммы вероятных потерь в случае вероятной информационной атаки.

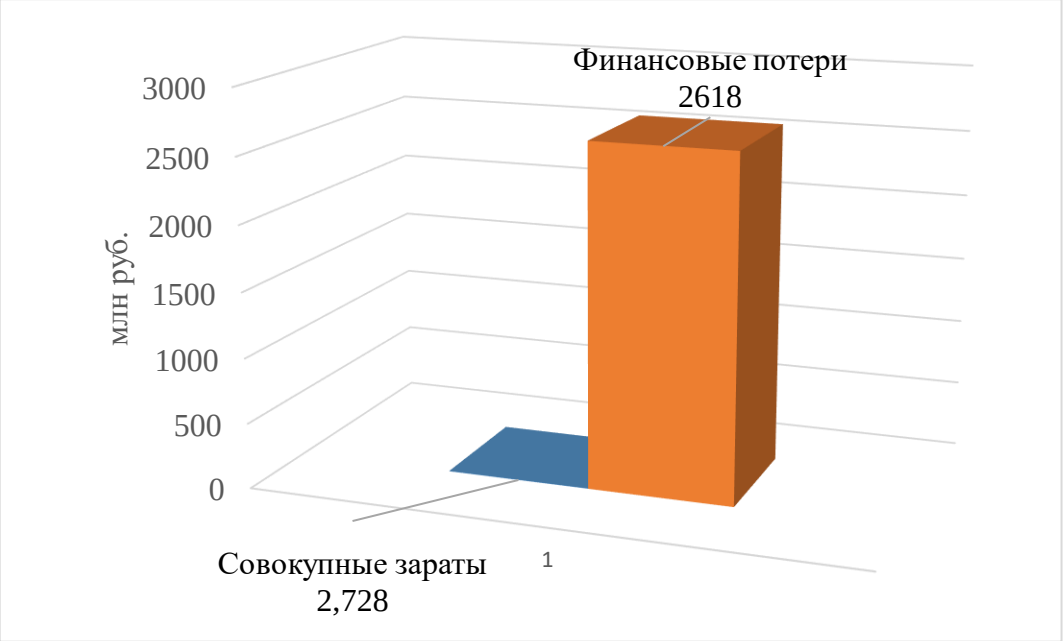


Рисунок 22 – Сравнение затрат на реализацию мероприятий по повышению информационной безопасности и суммы возможных потерь

«Для оценки эффективности мероприятий необходимо оценить какую часть от стоимости информации, циркулирующей на предприятии, составили затраты на проведение мероприятий». [12]

«Долю от стоимости информации рассчитывается по формуле (2):

$$P = (C_з \cdot 100) / C_{инф}, \quad (2)$$

где Р – доля от стоимости информации, циркулирующей на предприятии;

$С_з$ – стоимость затрат на проведение мероприятий;

$С_{инф}$ – стоимость информации, циркулирующей на предприятии» [12].

В исходную формулу подставляем необходимые значения и получаем:

$$Р = (2728200 \cdot 100) / 7040000000 = 3{,}16\ \%.$$

На реализацию всех запланированных работ было потрачено 2 728 200 руб., что составляет 3,16 % от стоимости информации, циркулирующей на предприятии, и это «соответствует принципу разумной достаточности» [12].

Для расчета экономической эффективности проведенных мероприятий составлена таблица 11.

Таблица 10 – Исходные данные расчета экономической эффективности мероприятий

Показатели	Единица измерения	Условные обозначения	Значения показателей
«Среднесписочная численность работников» [12]	чел.	$Ч_{исх}$	2474
«Среднемесячная заработная плата» [12]	руб.	$З_{мес}$	80 000
«Уровень отчисления на социальные нужды» [12]	%	$У_{ос}$	30
«Условно-постоянные затраты» [12]	руб.	$З_{уп}$	190 000
«Единовременные затраты, связанные с внедрением мероприятий» [12]	руб.	$З_{ед}$	415 000

Продолжение таблицы 10

Показатели	Единица измерения	Условные обозначения	Значения показателей
«Дополнительные капитальные вложения» [12]	руб.	$К_{доп}$	2 333 200
«Нормативный коэффициент эффективности» [12]	-	$Е_н$	0,3
«Трудоемкость производственного цикла» [12]	мин	$Т_1$	60
«Проектируемая трудоемкость производственного цикла» [12]	мин	$Т_2$	46

«Снижение трудоемкости производственного цикла рассчитывается по формуле (3):

$$T = (T_1 - T_2) / T_1 \cdot 100» [12] \quad (3)$$

$$Т = (60 - 46) / 60 \cdot 100 = 23,3 \%$$

«Прирост производительности труда администратора на основе снижения трудоемкости, %, равен:

$$\Delta П_с = (100 \cdot Т) / (100 - Т)» [12] \quad (4)$$

$$\Delta П_с = (100 \cdot 23,3) / (100 – 23,3) = 30,38 \%.$$

«Прирост производительности труда по предприятию, %, равен:

$$\Delta П_п = 1 / Ч_{исх} \cdot \Delta П_с» [12] \quad (5)$$

$$\Delta П_п = 1 / 2474 \cdot 30,38 = 0,12 \%.$$

«Условное высвобождение численности работников, чел:

$$\Delta Ч= (Ч_{исх} \cdot \Delta П_п) / (100 + \Delta П_п)» [12] \quad (6)$$

$$\Delta Ч= (2474 \cdot 0,12) / (100 + 0,12) = 2,96.$$

«Экономия в результате уменьшения отчислений на заработную плату, руб.:

$$Э_{з/п} = [\Delta Ч \cdot З_{мес} \cdot (1 + У_{ос} / 100)] \cdot 12» \text{ [12]} \quad (7)$$

$$Э_{з/п} = [2{,}96 \cdot 80000 \cdot (1 + 30 / 100)] \cdot 12 = 3\,694\,080.$$

«Экономия в результате относительного сокращения условно-постоянных затрат, руб.:

$$Э_{уп} = З_{уп} \cdot \Delta П_п / 100» \text{ [12]} \quad (8)$$

$$Э_{уп} = 190000 \cdot 0{,}12 / 100 = 228.$$

«Экономия условно-годовая, руб:

$$Э_{уг} = Э_{з/п} + Э_{уп} - З_{ед}» \text{ [12]} \quad (9)$$

$$Э_{уг} = 3\,694\,080 + 228 - 415\,000 = 3\,279\,308.$$

«Срок окупаемости, лет:

$$Т_{ок} = К_{доп} / Э_{уг}» \text{ [12]} \quad (10)$$

$$Т_{ок} = 2\,333\,200 / 3\,279\,308 = 0{,}7 \text{ г.}$$

Рассчитанная окупаемость средств, вложенных в повышение защиты информации, составляет 9 месяцев.

5.2 Оценка состояния системы безопасности информации по результатам проведения разработанных мероприятий

После проведения экономического анализа эффективности внедренных мероприятий повторно проанализируем частные показатели, характеризующие степень реализации отдельных мер по обеспечению безопасности от актуальных угроз. Результаты исследования показаны на рисунке 23. На рисунке приведены только показатели, значение которых улучшено после осуществления запланированных работ.

Номер группы показателей (i)	Наименование групп показателей	Наименование показателей	Значение частного показателя (Kji)	Значение весового коэффициента группы показателей (Rj)
1	Организация и управление	1.1 На заместителя руководителя организации возложены полномочия ответственного лица за обеспечение информационной безопасности организации и определены его обязанности	0,30	0,10
2	Защита пользователей	2.2 Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)	0,30	0,25
		2.4 Отсутствуют активные учетные записи работников организации, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,20	
3	Защита информационных систем	3.1 На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4	0,20	0,35
4	Мониторинг информационной безопасности и реагирование	4.3 Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25	0,30

Рисунок 23 – Коэффициенты показателей надежности после проведенных мероприятий

В результате расчета показателя надежности $К_{зи}$ получаем, что $К_{зи} = 1$. При этом значении показателя обеспечивается «минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)» [13, п.35].

На рисунке 24 показан график зависимости показателя текущего состояния защищенности ($К_{зи}$) от значения частных показателей (i) после проведенных мероприятий.

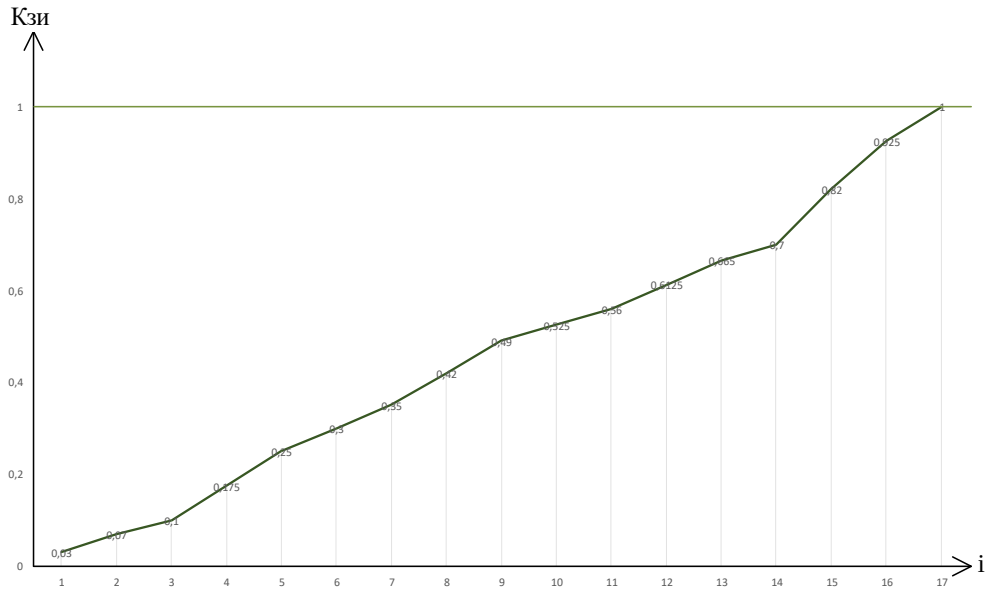


Рисунок 24 – График зависимости показателя текущего состояния защищенности ($К_{зи}$) после проведенных мероприятий

Следовательно, проведенные мероприятия позволили повысить уровень показателя текущего состояния защищенности информационных ресурсов предприятия до единицы.

На основе результатов оценки значений частного показателя построена диаграмма распределения данных показателей (рисунок 25). На ней красным цветом изображена диаграмма до проведения мероприятий по повышению информационной безопасности, зеленым – после. Как видно из рисунка, на вновь

построенной диаграмме отсутствуют нулевые значения коэффициентов. Уровень угроз, представленных в таблице 7, существенно снижен.

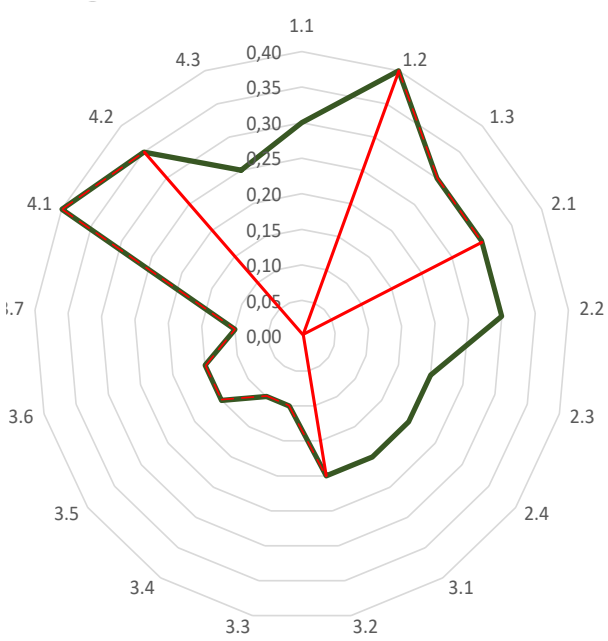


Рисунок 25 – Диаграмма распределения показателей безопасности после проведения мероприятий

Результаты повторной оценки показателя защищенности показали, что выполнение всех мероприятий по совершенствованию системы защиты информации дало возможность перейти предприятию с уровня - «защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации, уровень защищенности характеризуется как критический («красный»), на обеспеченный минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)». [13, п. 35]

В пятой главе были рассчитаны экономические затраты предприятия, обусловленные выполнением мероприятий для повышения состояния технической защиты информации, и сделан вывод о результативности их внедрения.

Заключение

Проанализировав результаты, полученные после проведения повторной оценки показателя защищенности, можно сделать вывод, что осуществленные мероприятия совместно с материальными затратами, выделенными на переоборудование информационной инфраструктуры АО «Нител», обеспечили минимальный уровень защиты от типовых актуальных угроз безопасности информации на предприятии и повысили информационную безопасность предприятия.

Для совершенствования системы информационной безопасности на предприятии были применены:

- аппаратный метод защиты информации использован в качестве организации двухфакторной аутентификации – использование USB флеш-накопителей;
- организационный метод – разработка Регламента по реагированию на компьютерные инциденты и усиление административной ответственности;
- программный метод – формирование рассылки информации отдела кадров для отдела безопасности с данных об увольнениях сотрудников предприятия для исключения их учетных записей из корпоративной сети предприятия;
- организационно-программный метод – разработка матрицы доступа ведущих специалистов предприятия к служебной информации, разработка и исследование модели оценки влияния обновлений иностранного программного обеспечения на информационную безопасность предприятия.

В процессе прохождения практики я приобрел навыки работы с документами ФСТЭК, изучил информационную систему предприятия, для оценки безопасности обновлений иностранного программного обеспечения была

разработана и апробирована модель их тестирования. В результате расширения видов электронных документов на предприятии я изучил существующие матрицы доступа к информации и разработал матрицу доступа к служебной информации. Для структурирования работы при обнаружении информационных атак был разработан Регламент реагирования на них. Все выполненные мной работы позволили значительно повысить мои знания в области обеспечения информационной безопасности на предприятии, которые существенно помогут мне в дальнейшей профессиональной деятельности.

Задача исследовательской работы – разработка современных моделей защиты информации на основе существующих методов и их использование в системе обеспечения информационной безопасности предприятия выполнена, это показано достижением минимального уровня «защиты от типовых актуальных угроз безопасности информации».

Практическая значимость работы определяется тем, что ее результаты позволили обеспечить надлежащую степень защищенности информационной безопасности в корпоративной сети предприятия путем использования разработанных моделей и предложенных методов, направленных на снижение информационных рисков. Результаты проведения повторной оценки показателя защищенности показали, что проблема повышения информационной безопасности предприятия до необходимого минимального полностью решена.

Организация информационной безопасности – это не раз и навсегда созданная и отлаженная структура. Разные ее части меняются как в процессе разработки, так и при функционировании. Необходимо «периодически проводить анализ рисков в области информационной безопасности и внедренных мероприятий по управлению информационной безопасностью для того, чтобы учесть:

- изменения требований и приоритета бизнеса;
- появления новых угроз и уязвимостей;
- снижение эффективности существующих мероприятий по управлению информационной безопасностью» [17, Введение].

Список используемой литературы и используемых источников

1 Вострецова Е.В. Основы информационной безопасности. Учебное пособие. Екатеринбург: Изд-во Урал. Ун-та, 2019. - 204 с.

2 Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. - СПб: НИУ ИТМО, 2011.- 112 с.

3 Государственный стандарт Российской Федерации ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта РФ от 9 февраля 1995 г. № 49) [Электронный ресурс] URL: http:// base.garant.ru> Государственный стандарт Российской Федерации ГОСТ … (дата обращения: 28.09.2024).

4 Дудко Д. Защита информации от утечек в ИТ-сети предприятия / «Системы безопасности». 2023. № 1. С. 120-121.

5 Егошин Н.С., Конев А. А., Шелупанов А.А. Формирование модели нарушителя / Безопасность информационных технологи. Том 24, № 4 (2017)

6 Егошин Н.С. Модели нарушения безопасности информационных потоков в киберпространстве. Автореферат. [Текст] [Электронный ресурс] URL: http: // dissercat.com> Модели нарушения…(дата обращения: 6.10.2024).

7 Ермилова Л., Грязнов А. Контроль над правами: как управлять привилегированными учетными записями /Информационная безопасность». – 2023. № 1. С. 16-17.

8 Информационная безопасность / Группа компаний Бизнес…. URL: http: // ооо-бизнес-решения> business-solution /…(дата обращения: 15.01.2025).

9 Келдыш Н.В. Системная защита информации компьютерных сетей. Учебное пособие - М.: Мир науки, 2022. - Сетевое издание. Режим доступа: URL: http://izd-mn.com/PDF/43MNNNPU22.pdf (дата обращения: 22.10.2024).

10 Конявская С. Проблемы использования биометрии в качестве фактора аутентификации / Информационная безопасность». 2023. № 2. С. 32-35.

11 Конявская С. Реалии и проблемы многофакторной аутентификации /Информационная безопасность». 2023. № 3. С. 64-65.

12 Корнеев Н.В., Лосева В.В. Методические рекомендации по выполнению экономического раздела дипломного проекта: Москва: Спутник+, 2012, 138 с.

13 Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. ФСТЭК России 2 мая 2024 г.) [Электронный ресурс] URL: http:// base.garant.ru> ПРАЙМ > Документы ленты ПРАЙМ….(дата обращения: 28.09.2024).

14 Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021г.) [Электронный ресурс] URL: http:// base.garant.ru> ПРАЙМ > Документы ленты ПРАЙМ….(дата обращения: 28.09.2024).

15 Методические указания. Практикум по расчету себестоимости программного продукта и экономической эффективности внедрения. Учеб.-методич. Пособие. - Невинномысск: НТИ (филиал) СКФУ 2021.- 68 с.

16 Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс] URL: http:// base.garant.ru> Национальный стандарт РФ ГОСТ Р 50922-2006 « Защита и…» (дата обращения: 28.09.2024).

17 Национальный стандарт РФ ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» [Электронный ресурс] URL: http:// rostest.info> gost/001.001.040.001/ gost-r-… (дата обращения: 06.10.2024).

18 Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27

декабря 2007 г. № 513-ст) [Электронный ресурс] URL: http: // base.garant.ru> Национальный стандарт РФ ГОСТ Р ИСО/МЭК…(дата обращения: 16.10.2024).

19 Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст) [Электронный ресурс] URL: http:// base.garant.ru> Национальный стандарт… (дата обращения: 16.11.2024).

20 Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб.: Изд-во СПбГЭУ, 2019. – 103 с.

21 Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления атомной энергии и уполномоченном органе при космической деятельности» (с изменениями и дополнениями) [Электронный ресурс] URL: http: base.garant.ru> Постановление правительства …(дата обращения: 16.12.2024).

22 Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» Утверждено решением председателя Государственной технической комиссии при президенте Российской федерации от 30 марта 1992 г. [Электронный ресурс] URL: http: base.garant.ru> Руководящий документ «Автоматизированные системы…» (дата обращения: 16.11.2024).

23 Рычков Д.В. Информационная безопасность на производстве: проблемы и решение / Главный инженер. 2019. № 11. С. 14 - 23.

24 Саматов К. Актуальные вопросы защиты КИИ в 2025 году /Информационная безопасность». 2024. № 6. С. 38-39.

25 Сколько стоят услуги программиста: стоимость 1 часа работы. [Электронный ресурс] URL: http: kadrof.ru> articles/46641 (дата обращения: 10.02.2025).

26 Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспертному контролю» (с изменениями и дополнениями) [Электронный ресурс] URL: http: base.garant.ru> 12136635/…(дата обращения: 10.19.2024).

27 Управление рисками: обзор употребительных подходов. URL: http: // infosecportal.ru > stati/upravlenie-riskami-obzor…. (15/01)

28 Пуха В., Половинко В. Изоляция как стратегия: однонаправленные шлюзы для промышленного сегмента сети /Информационная безопасность». 2024. № 6. С. 44-45.

29 Число кибератак на российские компании за год выросло URL: http: secret.tinkoff.ru> novosty/kiberataky-2024

30 Шпаков А. Решения Рутокен для аутентификации в российские ОС и информационные системы /Информационная безопасность». 2024. № 5. С. 52-53.

31 By Kusum Saini. Home Resources Cyber Security 20 Emerging Cybersecurity Trend to Watch Out in 2025 // Cyber Security Article / Simplilearn. URL: http: // simplilearn.com> Cyber Security> Article (дата обращения: 14.01.2025).

32 Bjorn Lundgren, Niklas Moller. Deffing Information Security URL: http: // link.springer.com> Science and Engineering Ethics> Article (дата обращения: 12.01.2025).

33 Godovoe-issledovanie-2023 // URL: http: // searchinform.ru > upload/sites/1/2024/03/….(дата обращения: 14.01.2025).

34 Jim Holdsworth, Matthew Kosinski. What is Information Security? IBM URL: http: // ibm.com> think/topics/ information-security… (дата обращения: 12.01.2025).

35 Md Obaidur Rahaman. Data and Information Security in Modern World // URL: http: // article.sapub.org> 10.5923.j.computer.20170701… (дата обращения: 14.01.2025).

36 Nick Batney. What is Autentification? | Definition from TechTarget URL: http: // techtarget.com>searchsecurity/definition/... (дата обращения: 12.01.2025).