АКАДЕМИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ КАЗАХСТАН

Институт управления

на правах рукописи

Абилов Адиль Манарбекович

ВНЕДРЕНИЕ DLP-СИСТЕМЫ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ

Образовательная программа «7М04105 - Государственная политика»
по направлению подготовки «7М041 Бизнес и управление»

Магистерский проект на соискание степени
магистра бизнеса и управления
«7М04105 - Государственная политика»

Научный руководитель: _____ Медебаева А.Б., доктор PhD

Проект допущен к защите: «___» _____ 2023 г.

Директор Института управления: _____ Гаипов З.С, д.п.н.

Астана, 2023

СОДЕРЖАНИЕ

Нормативные ссылки

В настоящем магистерском проекте использованы ссылки на следующие нормативные документы:

«План нации - 100 конкретных шагов» Программа Президента Республики Казахстан от 20 мая 2015 года.

Указ Президента Республики Казахстан от 15 февраля 2018 года № 636 «Об утверждении Национального плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан».

Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации».

Закон Республики Казахстан от 16 ноября 2015 года № 401-V ЗРК «О доступе к информации»

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")».

Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

Обозначения и сокращения

РК	–	Республика Казахстан
МИИР	–	Министерство индустрии и инфраструктурного развития
МЦРИАП	–	Министерство цифрового развития и аэрокосмического промышленности
ЦА	–	Центральный аппарат
ЕТС	–	Единая транспортная среда
ГО	–	Государственный орган
ЦА	–	Центральный аппарат
ПК	–	Персональный компьютер
СКУД АСП	–	Система контроля и управления доступом
ИБ	–	Информационная безопасность
ДАР	–	Департамент административной работы
ДКР	–	Департамент кадровой работы
ЖКХ	–	Жилищно-коммунальное хозяйство
в т.ч.	–	в том числе
и т.д.	–	и так далее

Введение

Актуальность темы исследования. Видение модели государственной службы заключается в профессионализации системы государственной службы, основанная на принципах меритократии, эффективности, результативности, транспарентности и подотчетности обществу, является важнейшим фактором в обеспечении конкурентоспособности системы государственного управления и качественного оказания государственных услуг населению. [1]

Вместе с этим, внедрение и развитие цифровых технологий способствуют большей прозрачности и подотчетности в государственном управлении. Цифровые решения позволяют адаптироваться и быстро реагировать на изменяющиеся обстоятельства и возникающие вызовы. Государственные служащие могут использовать эти цифровые инструменты для совершенствования бизнес процессов и достижения лучших результатов.

Всем известно, что с помощью цифровых технологий возможно достичь экономии средств и оптимизации ресурсов в государственном управлении. Автоматизация сокращает ручной труд, устраняет избыточность и сводит к минимуму потребность в физической инфраструктуре.

Когда государственные служащие эффективны, они могут предоставлять населению более качественные услуги. Это приводит к повышению удовлетворенности и доверия к правительству. Эффективные государственные служащие способны лучше обрабатывать информацию и быстро принимать решения. «Безынициативные, равнодушные чиновники на государственной службе не нужны» такое заявление сделал на расширенном заседании Правительства Глава Государства Касым-Жомарт Токаев. [2]

Цель и задачи исследования. Целью исследования является повышение эффективности деятельности государственных служащих путем внедрения DLP-системы.

Реализация поставленной цели обусловливает решение следующих **задач**:

- изучить теоретические и технические аспекты DLP-системы в государственном управлении;
- изучить международный опыт применения DLP-систем;
- выявить проблемы внедрения DLP-системы на государственной службе;
- разработать рекомендации по использованию DLP-системы по повышению эффективности государственных служащих.

Объектом исследования эффективность государственных служащих.

Предметом исследования DLP система, способствующая максимизации эффективности государственных служащих.

Методы исследования. Методология основана на методах стратегического планирования, системного подхода и анкетирования.

Гипотеза. Использование DLP-системы повысит эффективность государственных служащих.

Практическая значимость. Рекомендации будут использоваться на государственной службе и будут нести рекомендательный характер.

Публикация. Актуальность и результаты исследования нашли отражение в международном научно-практическом журнале XIX глобальные науки и инновации 2023: Центральная Азия.

Обзор литературы

Раскроем основные теоретические аспекты в научных публикациях по теме магистерского проекта.

В исследовании А.А. Мелимова, З.В. Семенова рассматриваются этические и правовые основания внедрения DLP-систем. Авторы отмечают что, внедрение DLP-систем со строгими механизмами контроля может создать культуру подозрительности и недоверия среди сотрудников. Постоянный мониторинг может привести к снижению морального духа и удовлетворенности работой, поскольку сотрудники могут чувствовать, что каждое их действие тщательно проверяется, что потенциально влияет на их чувство автономии и мотивацию. В этой связи, авторы рассмотрели ряд законов, не противоречащих внедрению DLP – системы, и ряд плановых рекомендации для внедрения данной системы. [3]

Дубровина А.И., в своем исследование рассмотрела архитектуру взаимодействия DLP – системы с локальной сетью и интернетом. Автор отмечает важность обеспечения информационной безопасности и насколько облегчена работа специалистам ИБ благодаря DLP. Также, в исследовании подчеркивается актуальность предотвращения потери данных как важнейшего аспекта информационной безопасности. Системы DLP помогают выявлять и снижать риски, связанные с несанкционированным раскрытием, кражей или потерей конфиденциальных данных. DLP-системы позволяют своевременно обнаруживать и предотвращать потенциальные утечки данных. [4]

И. Г. Гниденко, И.В. Егорова провели исследование по критериям выбора DLP-системы. Авторы отмечают что, экономическая эффективность системы DLP является важным критерием. Это должно соответствовать бюджету организации так как к статьям расходов будет относиться не только сам продукт, а его лицензия, стоимость развертывания системы, техническая поддержка и обновление. [5]

В исследовании Кащеевой, М. А. рассмотрены функционирование DLP-систем в государственных организациях. Автором раскрыта сущность и область использования системы, рассмотрен IT рынок, предоставляющий данное цифровое решение. По результатам исследования автор рекомендует систему, которая легко масштабируемая способна удовлетворять текущие и будущие потребности государственной организации. DLP-систем должна быть достаточно гибкой, чтобы адаптироваться к меняющимся технологическим ландшафтам, бизнес-процессам и объемам данных. Также, отмечается совместимость и интеграция с существующей ИТ-инфраструктурой государственной организации, включая сетевую архитектуру, приложения и хранилища данных. Система DLP должна легко интегрироваться с этими системами, чтобы обеспечить бесперебойное внедрение и эффективное управление данными. [6]

В научной литературе встречаются различные исследования по повышению эффективности деятельности государственных служащих.

К примеру, в исследовании Бекмурзиева Х.М. мотивированные государственные служащие с большей вероятностью будут выполнять свои обязанности с энтузиазмом, усердием и целеустремленностью, что может привести к лучшему предоставлению государственных услуг, повышению производительности и повышению эффективности самой организации. Она освещает различные типы мотивации, которые могут влиять на поведение и результативность государственных служащих, включая внутреннюю и внешнюю мотивацию. «Внутренняя мотивация относится к внутренним факторам, которые управляют поведением индивида, таким как личные интересы, ценности и убеждения, в то время как внешняя мотивация относится к внешним факторам, таким как вознаграждение, признание и продвижение по службе». [7].

В другом исследовании, А.А. Адаменко, Н.А. Гончарова и Е.А. Черкалин считают, что, эффективность трудоспособности зависит напрямую от удовлетворенности проделанной работы, а также на другие экономические результаты деятельности. «Для эффективности трудоспособности необходимы хорошо организованные условия работника». Авторы полагают что, основной формой стимулирования персонала все-таки является материальное вознаграждение, но, нематериальное стимулирование, является самой надежной так как высокий уровень нематериальных ценностей позволяют удерживать специалистов, или получить от них поддержку в кризисной ситуации. Отношения внутри коллектива формируются через нематериальную систему стимулирований. [8].

Исследование, проведенное, А.В. Скидан, Ю.А. Чипига и А.А. Исюк предлагают смену методов оценки эффективности деятельности государственных органов – «переход от бинарной оценки «выполнено – не выполнено» к применению предиктивной аналитики, то есть выборочных испытаний, основанных на технологиях искусственного интеллекта». [9].

В научной статье Э.Р. Бирюковой понятие «эффективность» в государственном управлении рассматривается как используются имеющиеся ресурсы субъектом государственного управления для решения обществом задач и достижения результатов.

В целом, проведенный обзор литературы по исследуемой теме свидетельствует о том, что повышение эффективности государственных служащих требует многогранного подхода, который включает в себя предоставление соответствующих стимулов, развитие лидерства и менеджмента, обучение коммуникациям и цифровизацию.

Методы исследования

Для достижения цели в магистерском проекте и проверки гипотезы рассмотрим подробнее использованные методы исследования.

Метод анкетирования.

− количественный метод. Данного рода опрос должен показать реальную позицию государственных служащих по внедрению DLP-системы и определить основные показатели эффективности сотрудника. Социологический опрос был проведен среди 47 государственных служащих Министерства индустрии и инфраструктурного развития РК, в период с 7 по 12 апреля. Опросник составлен на платформе Google, далее посредством социальных сетей и электронной почты была предоставлена возможность прохождения данной анкеты. Опросник состоит из 9 закрытых и открытых вопросов. Обработка и результаты социологического опроса представлены в разделе анализа исследования.

− качественный метод. С помощью глубинного интервью проведен сбор данных и мнения экспертов. Состоялось глубинное интервью на русском языке с 8 руководителями Центрального аппарата Министерства индустрии и инфраструктурного развития РК.

Таблица 1 − Вопросы глубинного интервью

№	Вопрос	Цель
1	Удовлетворены ли вы уровнем эффективности своих сотрудников?	Узнать общую среднюю оценку уровня удовлетворенности эффективности работы сотрудников.
2	Какие инструменты вы практикуете для повышения их эффективности в работе?	Узнать о проводимой работе руководства по повышению эффективности своих подчиненных.
3	По какой системе осуществляется распределение премий (бонусов) между сотрудниками в департаменте?	Изучить методику распределения премий в коллективе.
4	Контролируете ли Вы своих сотрудников во время удаленного режима работы?	Узнать мнение руководства о необходимости мониторинга во время удаленного режима работы.

Продолжение таблицы 1

1	2	3
5	Как вы определяете степень загруженности своих сотрудников перед распределением поручений?	Сравнить используемые методы со стороны руководства во время распределений задач.
6	Какие меры принимаются в отношении сотрудников, которые задерживаются на работе?	Узнать практический опыт дисциплинарных мер.
7	Знаете ли вы о функциональных возможностях DLP-системы?	Исследовать уровень осведомленности о DLP-системе.
8	Как вы оцениваете предоставляемые служебные компьютеры вашим сотрудникам для работы?	Оценить технические возможности для внедрение DLP-системы.
9	По вашему мнению насколько этично было внедрять DLP-систему в Центральном аппарате министерства?	Узнать уровень сопротивления внедрения DLP-системы.
10	Готовы ли вы распределять премии (бонусы) между сотрудниками по результату автоматического отчета из DLP-системы?	Узнать мнение руководства о готовности эксплуатации системы.
11	Будете ли вы наблюдать за действиями сотрудника в служебном компьютере через DLP-систему во время удаленного режима работы?	Узнать мнение руководства о готовности эксплуатации системы.
12	Ваши рекомендации по использованию DLP-системы с целью повышения эффективности ваших сотрудников?	Собрать предложения по улучшению системы и новых возможностях повышения эффективности сотрудников.
Примечание – составлено автором для проведения экспертного интервью		

Далее, для всестороннего анализа внедрения DLP-системы использовался метод SWOT-анализа, по результатам данного метода удалось рассмотреть внедрение системы с различных сторон.

Также, проведено исследование международного опыта применения DLP-систем как в частном так и в государственном секторе.

Исследование, базировалось на трех основных этапах: 1 этап. Обзор и исследование литературных источников по вопросам повышения эффективности деятельности государственных служащих и использование цифровых решение в кадровой работе. 2 этап. Проведение количественного и качественного анализа, изучения международного опыта действующей практики по вопросам повышения эффективности деятельности государственных служащих с использованием цифровых решений. 3 этап. Разработка практических рекомендаций с использованием DLP-системы.

Анализ и результаты исследования

Функциональный анализ DLP-системы. Рассмотрим административную панель DLP-системы, которая состоит из 8 модулей на рис.1.

Рисунок 1 − Панель администратора
Примечание - предоставлено разработчиками продукта

Функциональные возможности модулей:

1 модуль «Поиск информации»:

- быстрый поиск информации на служебных компьютерах сотрудников по набору одного слова или нескольких тезисов;
- мониторинг сотрудников в рамках служебного расследования;
- определение деструктивных сотрудников;
- автоматическое определение взаимосвязи между сотрудниками;
- просмотр даты и методы хранения информации в т.ч. секретной;

2 модуль «Комбинированный поиск»:

- точная настройка поиска информации;
- запрос на совпадение текстового содержимого на всех участках;
- создание комбинаций условий поиска.

3 модуль «Мониторинг файловых систем»:

- выявление несанкционированного хранения в т.ч. передача электронной информации для служебного использования.

4 модуль «Активность пользователей»:

- общий мониторинг хронометража сотрудника (рис. 2);
- просмотр распечатанных документов;
- аудио или видео подключение к компьютеру сотрудника;
- мониторинг рабочего стола служебного компьютера:
- проведение анализа дублирующихся функций между Департаментами;
- просмотр ввода с клавиатуры (кейлоггер), добавления информации в буфер обмена, выгрузки из него.

Рисунок 2 − Формирование хронометража рабочего дня в DLP

Примечание - предоставлено разработчиками продукта

5 модуль «Отчёты»:

- формирование детальных отчетов о рабочем дне сотрудника и оценка его продуктивности в программах в т. ч. используемых в ЕТС ГО (рис. 3);
- построение схем связей – между сотрудниками внутри Министерства или с третьими лицами.

Рисунок 3 − Отчет по пользователю
Примечание - предоставлено разработчиками продукта

6 модуль «Политика безопасности»:

- настройка правил безопасности и отправки уведомлений о нарушении правил;
- настройка групповой политики;

7 модуль «Расследования»:

- обобщение и анализ материалов и вовлеченных лиц по инцидентам и служебным расследованиям;
- формирование дела для документального оформления и представить в виде доказательств в суде или ином разбирательстве.

8 модуль «Анализ рисков»:

- формирование модели поведения сотрудников с присвоением соответствующего уровня риска;
- анализ финансовых и репутационных рисков;
- сообщение о частых перемещениях между папками на компьютере, копирование на съемные носители;
- блокировка usb портов для всех ПК подключенных к DLP-системе.

Итак, для достижения цели магистерского проекта рассмотрев технические возможности вышеперечисленных модулей, определяем фокус инструменты для дальнейшей работы:

- Модуль «Отчёты»;
- Модуль «Политика безопасности»;
- Модуль «Расследования»

Через модуль отчетности имеется возможность получать сведения о продуктивности такие как: начало рабочего дня, переработка, среднее время активности часов в сутки. Эти данные формируются автоматически по заданному интервалу времени в формате excel, что позволит руководству структурного подразделения следить за физическим состоянием своих сотрудников, тем самым повышая их эффективность работы. В таблице 2. показан образец по форме данного отчета для руководства.

Таблица 2 – Отчет в разрезе сотрудников

	Среднее время начала работы	Среднее время окончания работы	Время активной работы пользователя за ПК	
Пользователь	n̄	n̄	n̄	∑n
Сотрудник 1	08:52:12	19:50:24	04:37:58	23:09:54
Сотрудник 2	07:43:12	19:54:48	04:54:24	24:32:02
Сотрудник 3	08:42:00	17:58:15	04:02:50	16:11:23
Сотрудник 4	08:26:12	18:10:00	02:58:26	14:52:11
Сотрудник 5	08:15:36	18:21:00	03:50:37	19:13:07
Сотрудник 6	09:05:48	19:46:24	07:07:01	35:35:07
Сотрудник 7	09:13:24	19:16:00	02:22:58	11:54:52
Сотрудник 8	10:02:24	18:05:48	02:47:13	13:56:08
Сотрудник 9	08:56:00	18:53:24	04:50:49	24:14:07
Сотрудник 10	09:10:36	18:20:24	03:20:33	16:42:47
Сотрудник 11	08:35:48	17:04:12	05:20:48	26:44:03
Примечание - выгрузка из DLP-системы за неделю				

Исходя из данной выгрузки можно заметить, что по включению и отключению служебных компьютеров выявляются сотрудники, которые опоздали на работу, переработали или вовсе покинули рабочее место раньше завершения рабочего дня.

Столбец «Время активной работы пользователя за ПК» где n̄, отражает активную продуктивность за день, ∑n – итого, за неделю.

Благодаря модулю «Политики безопасности» имеется возможность настроить групповую политику служебных компьютеров Министерства.

Данная настройка позволит автоматически отключать служебные компьютеры по завершению рабочего дня, что положительно скажется на эффективности работы, так как снизится показатель переработки и задержки на работе. Сотрудник адаптируется не откладывать задачи и решать их более оперативно, тем самым появится время для личной жизни и саморазвитию. В таблице 3. приводится настройка групповой политики.

Таблица 3 – Настройка групповой политики для отключения ПК

Шаг	Раздел	Команда/Путь
1	Настройка модуля «Политика безопасности»	Панель администратора
2	Подключение к домену Министерства и запуск оснастки управления групповой политики	Start — Control Panel — Administrative Tools — оснастка: Group Policy Management
3	Заходим до уровня Active Directory	Group Policy Management — Forest: polygon.local — Domain — Polygon.local
4	Создаем новую политику	на polygon.local → Create a GPO in this domain, and Link it here → GPO_Shutdown
5	Настройка созданного шаблона политики	На GPO_Shutdown → Computer Configuration — Preferences — Control Panel Settings — Scheduled Tasks → далее правый клик на пустом месте справа, New → Scheduled task
6	В появившемся окне Task выставляем следующие параметры	Action: Update Name: GPO_Shutdown Run: C:\Windows\system32\shutdown.exe Arguments: /s /c "ekonomim energy" /d p:0:0 Отмечаем пункт: Run As User Name: POLYGON\miir Password: A@off123ggg Confirm Password: A@off123ggg
7	Вкладка: Schedule	Указываем когда создаваемое задание прописанное групповой политикой на компьютерах локальной сети организации будет приведено в действие – 18:30 Scheduled Task: Daily Start Time: 18:30:00 PM Schedule Task Daily: Every 1 days После нажимаем Apply и Ok

Продолжение таблицы 3

1	2	3
8	Перезагрузка всех ПК	Планировщик заданий: Пуск — Панель управления — Администрирование — Планировщик Заданий
9	Библиотека планировщика	Настроить время перезагрузки всех ПК GPO_Shutdown задать время
Примечание – предоставлено разработчиками системы		

Последний модуль «Расследования» позволит повысить эффективность сотрудников ДКР. Для проведения служебных расследований в данном модуле предоставлены функциональные возможности формирования дела и быстрого поиска необходимой информации на служебных компьютерах у сотрудников.

Далее, собрав необходимые сведения, сотрудник управления служебных расследований сможет истребовать более качественные объяснительные по данным фактам.

Изучив функциональных инструменты DLP - системы мы переходим к результатам социологического опроса и экспертного интервью с целью рассмотрения возможности использования DLP - системы для повышения деятельности государственных служащих.

Количественный метод.

В целях изучения путей повышения эффективности государственных служащих и определения основных показателей эффективности деятельности был проведен опрос действующих государственных служащих в количестве 47 респондентов. Опрос проводился в Центральном аппарате Министерства индустрии и инфраструктурного развития РК. В таблице 4 сформирована первоначальная информация о сотрудниках МИИР РК.

Таблица 4 – Информация о респондентах

№	Параметры	Ответы	Количество респондентов	% от общего количества
1	Возраст	20-25	3	6,4
		26-35	17	36,2
		36-54	25	53,2
		55-64	2	4,3

Продолжение таблицы 4

1	2	3	4	5
2	Выслуга лет	0-1	2	4,3
		1-3	6	12,8
		3-5	2	4,3
		5-10	13	27,7
		10 и выше	24	51,1
Примечание – составлено автором по результатам опроса				

Далее, для внедрения DLP - системы у респондентов выяснили текущий уровень удовлетворенности техническими характеристиками служебных компьютеров. Результаты ответов представлены на рис. 4.

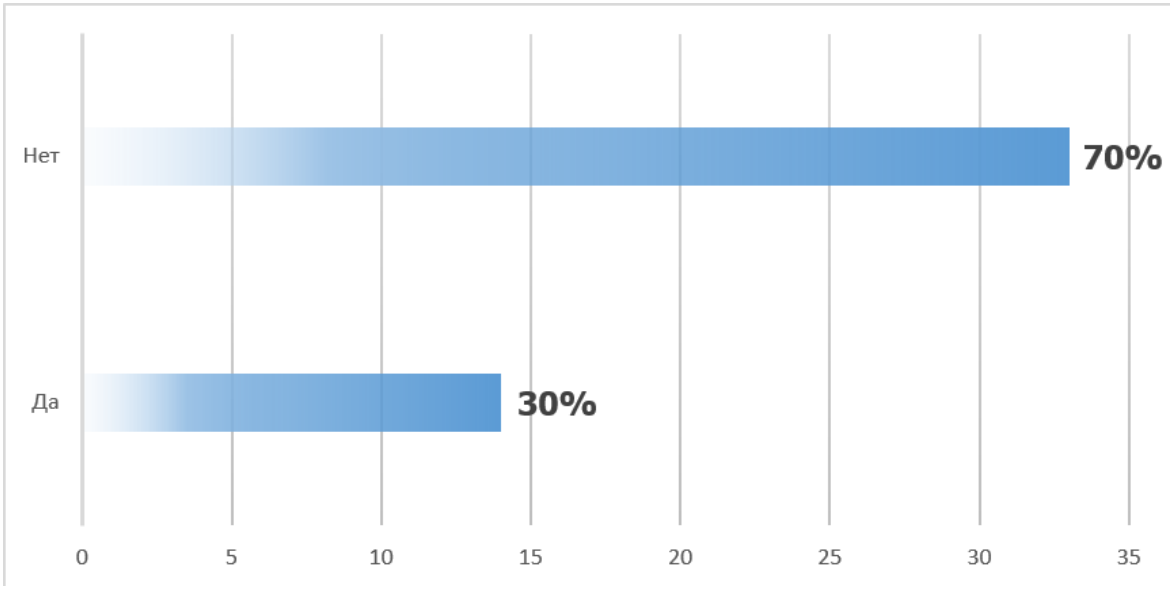

Рисунок 4 – Результаты опроса по уровню удовлетворенности тех.характеристиками служебных компьютеров

Примечание - составлено автором по данным опроса

В целом для надлежащего исполнения служебных обязанности требуется обновлять служебные компьютеры уровень амортизации которых составляет более 75%.

Учитывая технические требования для установки DLP-агента на служебные компьютеры достаточно минимальных требований, рекомендованных Microsoft для работы операционной системы.

В части распределения рабочего времени только у 28% респондентов установлен баланс между работой и личной жизнью. На рис. 5. представлены результаты данного опроса.

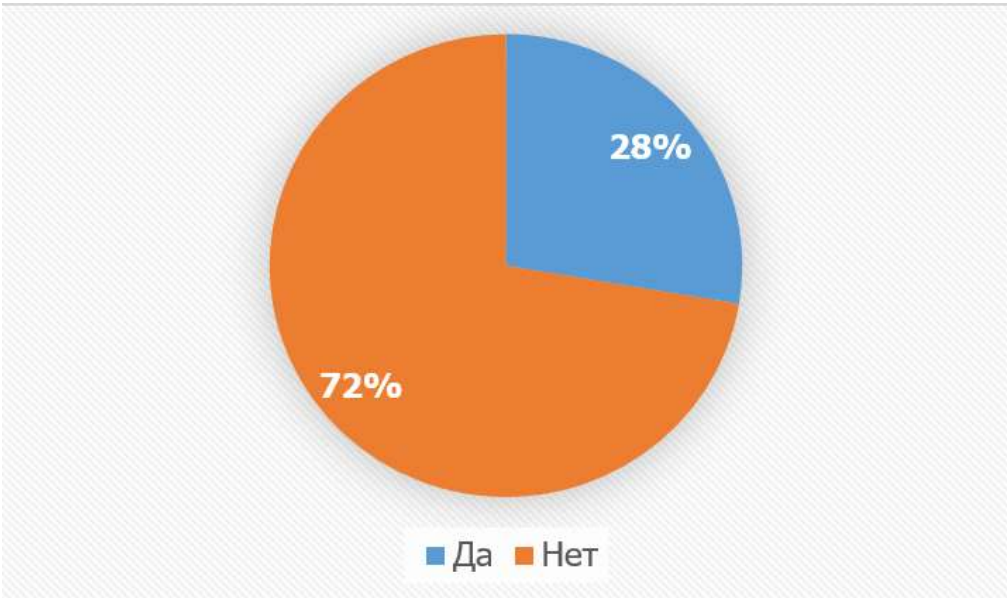

Рисунок 5 – Результаты оценки распределения рабочего времени
Примечание - составлено автором по данным опроса

Стоит отметить что, через групповую политику и её настройках через модуль политики безопасности в DLP - системе для эффективного контроля и распределения рабочего времени есть возможность использовать функцию отключения компьютеров по окончанию рабочего дня. (Таблица 3)

Рассмотрим основные показатели эффективности государственных служащих по результатам опроса на рис. 6.

Рисунок 6 – Результаты опроса по выбранным показателям эффективности

Примечание - составлено автором по данным опроса

Сотрудники министерства считают, что, наиболее эффективными сотрудниками являются в первую очередь обладающие такими компетенциями как ответственность, оперативность, умение принимать решения, ориентированность на достижение результата, умение сотрудничать и т. д.

Теперь в рамках данного исследования мы определили какие компетенции необходимо повышать для эффективной работы.

В целом, для руководящего состава DLP-система может стать дополнительным цифровым управленческим инструментом для повышения эффективности сотрудников, к примеру, можно вести мониторинг или сформировать автоматический отчет среди государственных служащих по эффективному распределению рабочего времени. Наблюдая за государственным служащим через DLP-систему у руководства будет возможность поддерживать организационную культуру в коллективе.

В рамках проводимого исследования следует также остановиться на мнении сотрудников об этичности внедрения DLP-системы и её установку в служебный компьютер, результаты приведены на рис. 7. и рис. 8.

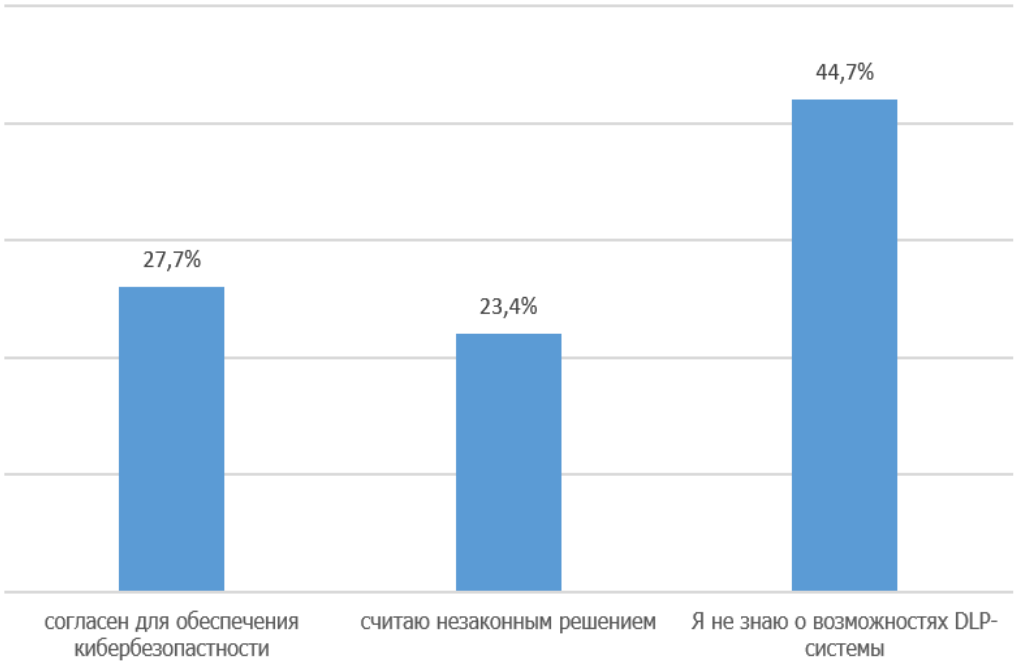

Рисунок 7 – Результаты опроса об этичности внедрения DLP-системы

Примечание - составлено автором по данным опроса

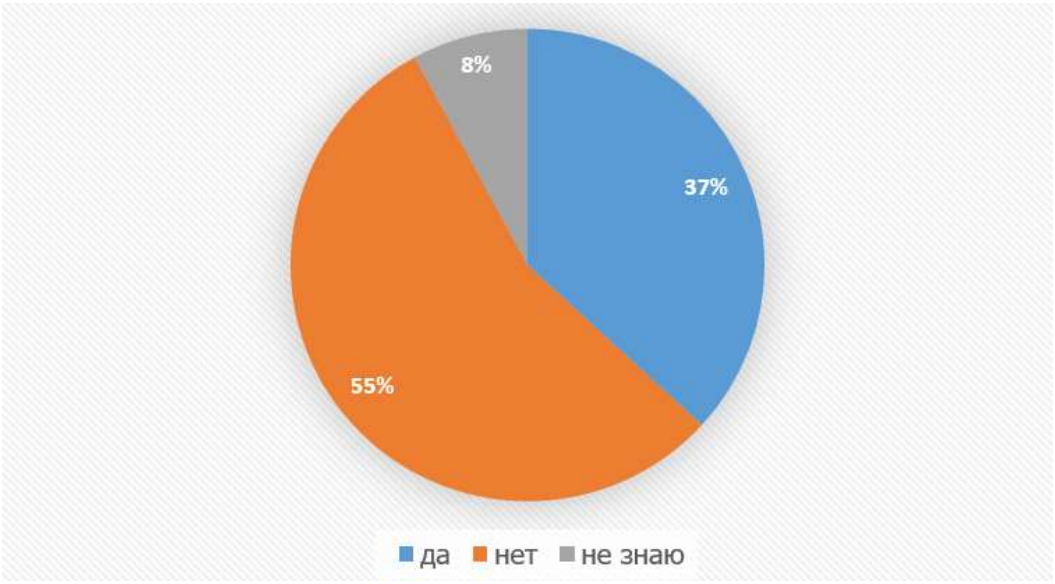

Рисунок 8 − Результаты опроса о согласии установки DLP-агента на ПК
Примечание - составлено автором по данным опроса

Из этих данных мы видим, что 44,7% респондентов не знают о функциональных возможностях DLP-системы и 55% государственных служащих не согласны с установкой DLP-агента на служебный компьютер.

Основные причины несогласия с установкой DLP-агента, респонденты указывают на слабую мощность служебных компьютеров и полагают что программа будет влиять на процессор ПК. Некоторые респонденты желают ознакомиться с функциональными возможностями DLP-системы перед тем как ее установят.

В этой связи, перед внедрением DLP-агента необходимо подготовить внутренний медиа-план по освещению вопросов внедрения DLP-системы в Министерстве с учетом разъяснительных процедур о влиянии программы на загрузку процессора.

Так как мало известно, что, на сегодняшний день в рамках Концепции кибербезопасности ("Киберщит Казахстана") для обеспечения кибербезопасности государственной системы уполномоченным органом осуществлена работа по внедрению DLP – системы «Киберстраж» в государственных органах.

Данную работу за счет средств уполномоченного органа реализовала Казахстанская IT компания MSSP.Global, по данным компании уже в 19 министерствах внедрена DLP - система.

Также, важно отметить об ответственности в нормативно-правовых актах регулирующие защиту и доступ к информации в законах РК.

К примеру, в законе «Об информатизации» в статье 56 установлено требование о принятие мер по защите данных содержащие персональные данные.

В то же время в законе «О доступе к информации» в 4 статье четко регламентируется принципы доступа к информации.

Вместе с этим, составлен операционный алгоритм установки (развертывания) DLP-системы. Проект алгоритма представлен на рис. 9.

Рисунок 9 – Операционный алгоритм установки DLP-системы.
Примечание - составлено автором во время прохождения практики в IT – холдинге KazDream

После прохождения этапа сбора информации и выделения средств необходимо учитывать системные требования серверного оборудования с количеством сотрудников. В таблице 5 приводятся системные требования.

Таблица 5 − Информация о системных требованиях.

Колл. рабочих станций	**ЦП**	**Сетевые адаптеры**	**Оперативная память**	**Системный диск**	**Диск для индексов**	**Диск для баз данных (6 месяцев)**
25	2,2+ ГГц (4 ядра и более)	1 Гбит (2 адаптера при использовании централизованного перехвата)	8GB+	200 GB	100 GB	256 GB
100	2,4+ ГГц (6 ядер и более)	1 Гбит (2 адаптера при использовании централизованного перехвата)	12 GB+	200 GB	250 GB	1024 GB

Продолжение таблицы 5

1	2	3	4	5	6	7
200	2,4+ ГГц (8 ядер и более)	1 Гбит (2 адаптера при использовании централизованн огоперехвата)	16 GB+	200 GB	400 GB	2048 GB
300	2,4+ ГГц (2 процессора по 6 ядер)	1 Гбит (2 адаптера при использовании централизованн огоперехвата)	24 GB+	200 GB	500 GB	3096 GB
500	2,6+ ГГц (2 процессора по 8 ядер)	1 Гбит (2 адаптера при использовании централизованн огоперехвата)	48 GB+	200 GB	1024 GB	5120 GB
1000	2,6+ ГГц (2 процессо ра по 12 ядер)	1 Гбит (2 адаптера при использовании централизованн огоперехвата)	96 GB+	200 GB	2048 GB	10240 GB
Примечание – составлено автором по источнику [11]						

Также, стоит отметить что на сервере баз данных DLP запрещено размещение баз, используемых другим ПО. При контроле более 500 пользователей обязательным условием является ежемесячное создание новой базы данных для каждого сервера перехвата и назначение ее в качестве хранилища для новых данных.

Используя инструменты проектного менеджмента по диаграмме Ганта стало известно, что, для завершения работ по внедрению DLP-системы потребуется 55 календарных дней (рис. 10).

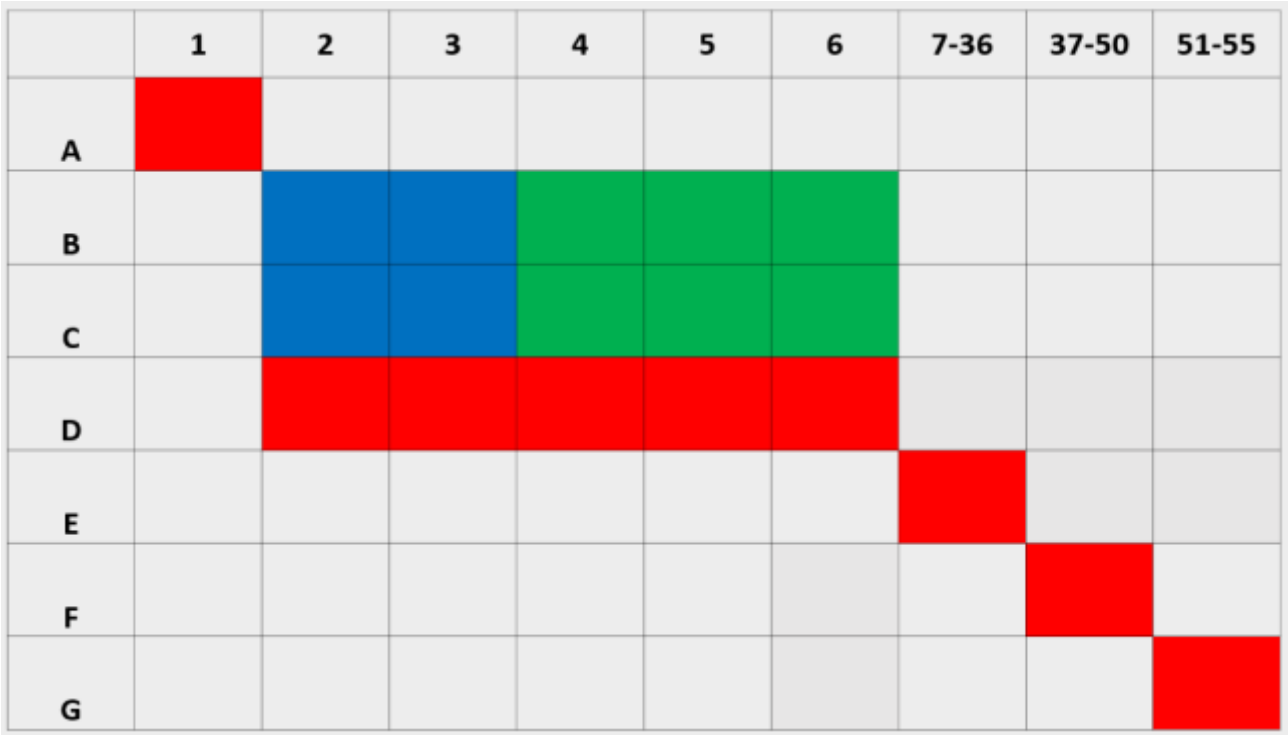

Рисунок 10 − диаграмма Ганта

Примечание - составлено автором по результатам таблицы 6

Таблица 6 − Основные этапы работ.

№	Работы	Прошедшая работа	Продолжительность работы
A	Старт	-	1
B	Запрос информации у ДАР	A	2
C	Запрос информации у ДКР	A	2
D	Подготовка бюджетной заявки	A	5
E	Технические работы	B,C,D	30
F	Запуск Агентов	E	14
G	Проверка установки	F	5
Примечание – составлено автором			

Из таблицы 6 у этапов работ самое продолжительное время занимают технические работы (30 дней) и централизованная установка DLP-агентов (14 дней).

Учитывая развитую цифровую архитектуру МИИР РК, где каждый компьютер, когда привязан к домену в локальной сети, с помощью консоли

администратора осуществляется единая централизованная установка DLP-агентов каждому сотруднику.

В случаях отсутствия сотрудников в локальной сети необходим контроллер домена. Таким образом, работоспособность контроллера домена влияет на возможность использовать всю IT-инфраструктуру государственного органа. Тем самым, после завершения внедрения DLP – системы, информация об активных действиях на служебном компьютере государственного служащего будет поступать через индивидуальный домен в DLP – консоль администратора.

По завершению социологического опроса мы получили следующие рекомендации и предложения по повышению эффективности государственных служащих:

- предусмотреть новые методы материального и нематериального стимулирования;
- внедрить метод установления сроков реализации поставленных задач, поручений от вышестоящего руководства;
- провести реинжиниринг бизнес-процессов;
- проводить квартальный анализ на наличие дублируемых документов и функций между управлениями;
- провести ревизию предоставляемых отчетов, т.е. сгруппировать их по степени важности и дальнейшего использования вышестоящим госорганом;
- отменить систему начисления заработной платы по факторно-бальной шкале.

Экспертное интервью.

В рамках глубинного интервью приняло участие 8 экспертов с Министерства индустрии и инфраструктурного развития РК, занимающие руководящие должности. По теме исследования от экспертов стало известно, что, средний уровень удовлетворенности эффективности своих сотрудников составляет 65%. При этом для повышения их эффективности в работе эксперты в основном используют только методы мотивации: материальные и не материальные сложившееся устоями времени и нормативно-правовыми актами для государственных служащих. Такие как, выплата бонусов, награждение грамотами, предоставление учебного отпуска. Лишь 2 эксперта связывают повышение эффективности сотрудников с важностью поддержания морально психологического климата в коллективе и совершенствования организационной культуры.

В отношении сотрудников, которые задерживаются на работе эксперты предоставляют отгулы в соответствии с Трудовым кодексом РК. Основная проблема почему сотрудники задерживаются на работе, эксперты считают, что, сотрудники не успевают обработать поступающую информацию и откладывают некоторые задачи под конец рабочего дня. В этой связи эксперты предлагают провести функциональный анализ в подразделениях, для выявления несвойственных функций и определения сотрудников с высокой степенью загруженности.

О функциональных возможностях DLP-системы известно всем экспертам, однако эксперты полагают что, не все сотрудники знают о возможностях DLP-системы и предлагают сделать паспорт проекта для раздаточной информации. Также, полагают что, внедрение DLP-системы должно приниматься коллегиально.

Касательно этичности внедрения DLP-системы системы, эксперты отмечают как положительные, так и отрицательные стороны системы. Эксперты предлагают при внедрении DLP-системы ограничить функции администратора, предоставлять доступ к системе ограниченный круг лиц так как система может сохранить информацию из личной жизни сотрудника.

Мнение экспертов по наблюдению за сотрудниками с помощью DLP-системы разделилось. Эксперты полагают, что во время удаленного режима работы — это необходимо, при этом отмечается ключевой фактор доверия.

Основные рекомендации и предложения экспертов по использованию DLP-системы:

- использовать DLP-систему для обеспечения ИБ;
- использовать систему для перераспределения штатной численности;
- доработать модуль «отчеты», добавить графу по выполненным работам, счетчик для учета потраченного времени на совещаниях и телефонных переговоров;
- провести интеграционные работы с системой СКУД, АСП;
- предоставление результатов системы сотрудникам;
- сформулировать критерии оценки для DLP-системы, для конкретного взаимопонимания между руководством и сотрудником;
- использовать преимущества системы для проведения служебного расследования.

Международный опыт.

Соединенные Штаты: Правительство США внедрило DLP-системы для повышения безопасности данных и предотвращения утечек информации в различных ведомствах. Например, Министерство обороны внедрило DLP-решения для защиты конфиденциальной информации и обеспечения соблюдения правил обработки данных. [12]

Также, с 2013 года Министерство внутренней безопасности США внедрило системы DLP для защиты критически важной инфраструктуры и конфиденциальных правительственных данных.

Правительство Великобритании внедрило системы DLP для защиты конфиденциальной информации и улучшения управления данными. Правительственные учреждения, такие как Министерство обороны и Министерство внутренних дел, внедрили DLP-решения для предотвращения утечек данных, управления контролем доступа и мониторинга использования данных. Усилинное развитие кибербезопастности началось с 2016 года, в общей сложности было выделено 2,38 млрд.долларов на 5 лет. [13]

Правительство Австралии признало важность систем DLP для защиты конфиденциальных данных в государственных учреждениях. Австралийское управление сигналов (ASD) предоставляет руководящие принципы и ресурсы, помогающие правительственным организациям эффективно внедрять DLP-системы. Основное внимание уделяется защите секретной информации, предотвращению утечки данных и соблюдению соответствующих правил конфиденциальности и безопасности. [14]

Правительство Сингапура внедрило DLP-системы в рамках своей общей стратегии кибербезопасности. Управление по развитию информационных технологий Infocomm Media Development Authority (IMDA) предлагает правительственным учреждениям рекомендации по внедрению DLP-решений для защиты конфиденциальных данных, предотвращения несанкционированного доступа и совершенствования методов защиты данных. Цель состоит в укреплении общей системы кибербезопасности и защите критически важной правительственной информации. [15]

Европейский союз поощряет внедрение систем DLP в правительственных учреждениях во всех своих государствах-членах. Общий регламент по защите данных (GDPR) содержит особые требования к защите данных, и системы DLP играют жизненно важную роль в обеспечении киберзащиты. Государства - члены ЕС, такие как Германия, Франция и Нидерланды, уже внедрили DLP-решения для защиты данных граждан и повышения информационной безопасности.

До 17 октября 2024 года государства-члены ЕС должны принять и опубликовать меры по кибербезопасности, необходимые для соблюдения Директивы по кибербезопасности NIS 2. [16]

Международный опыт применения DLP-систем в государственных учреждениях могут различаться в разных странах в зависимости от их уникальной нормативно-правовой базы, требований к защите данных и организационных потребностей. Однако их общая цель остается неизменной: защитить конфиденциальные правительственные данные, предотвратить утечку данных.

По результатам анализа международного опыта стало известно, что, функции мониторинга сотрудников, проведение служебных расследований и др. преимущественные функции не используются рядом передовых стран.

Очевидно, что для руководства в государственном секторе используя возможности DLP – системы будет дополнительным инструментом эффективного управления.

В рамках системного анализа выделяются основные секторы промышленности мировой экономики по применению DLP – систем:

Финансы. Банки и финансовые учреждения используют DLP-системы для защиты конфиденциальных данных клиентов, предотвращения финансового мошенничества и обеспечения соответствия нормативным требованиям. К примеру, DLP помогает отслеживать и контролировать передачу финансовых данных, таких как информация о кредитной карте или информация,

позволяющая установить личность, как внутри организации, так и внешним сторонам.

Здравоохранение. В секторе здравоохранения системы DLP используются для защиты данных пациентов, соблюдения требований HIPAA (в Соединенных Штатах) и защиты медицинских записей. DLP помогает обнаруживать и предотвращать несанкционированный доступ, снижать риск утечки данных и обеспечивать соблюдение политик конфиденциальности, регулирующих обработку конфиденциальной медицинской информации.

Образование. DLP-системы используются в образовательных учреждениях для защиты записей учащихся, исследовательских данных и интеллектуальной собственности. DLP помогает контролировать обмен конфиденциальной информацией, предотвращать плагиат и обеспечивать соблюдение политики защиты данных в академической среде.

Торговля и электронная коммерция. Розничные торговцы и платформы электронной коммерции используют DLP-системы для защиты платежных данных клиентов, предотвращения мошенничества с кредитными картами и защиты конфиденциальности клиентов. DLP помогает отслеживать потоки данных по различным каналам, включая онлайн-транзакции, электронную почту и передачу файлов, для обнаружения и предотвращения утечек данных и несанкционированного доступа.

Технологические компании. DLP применяется в технологических компаниях для защиты интеллектуальной собственности, коммерческой тайны и конфиденциальной деловой информации. DLP-системы помогают отслеживать перемещение данных по сетям, облачным хранилищам и инструментам совместной работы, гарантируя, что конфиденциальная информация остается в пределах разрешенных границ, и предотвращая утечку данных.

Юридические фирмы. Юридические фирмы используют DLP-системы для защиты клиентских данных, поддержания конфиденциальности и соблюдения правил защиты данных. DLP помогает предотвращать несанкционированное раскрытие конфиденциальных юридических документов, контролировать каналы связи и обеспечивать контроль доступа к данным.

Энергетика и ЖКХ. Системы DLP используются в секторе энергетики и ЖКХ для защиты критически важной инфраструктуры, конфиденциальных оперативных данных и интеллектуальной собственности. DLP помогает предотвращать несанкционированный доступ к системам управления, отслеживать потоки данных внутри сетей и обеспечивать соответствие отраслевым нормативам.

Для всестороннего рассмотрения вопроса по внедрению DLP-системы в государственном органе проведем **SWOT-анализ**.

Сильные стороны.

DLP-система помогают защитить конфиденциальные данные от несанкционированного доступа, потери или их утечки. Они отслеживают потоки данных как внутри государственного органа, так и по периметру сети, чтобы выявлять и предотвращать потенциальные утечки данных. Это обеспечивает

конфиденциальность секретной информации и соблюдение правил защиты данных.

Наряду с этим, DLP-системы используют усовершенствованные механизмы обнаружения для выявления потенциальных угроз безопасности данных. Они могут обнаруживать закономерности и аномалии в передаче, использовании и хранении данных, позволяя организациям заблаговременно устранять риски безопасности и предотвращать инциденты с потерей данных. Отечественный DLP-комплекс включен в реестр доверенного программного обеспечения и продукции электронной промышленности МЦРИАП, доверенный поставщик АО «Самрук Казына» и ТОО «Тенгизшевройл».

Действующий сертификат безопасности: СТ РК ГОСТ Р ИСО/МЭК 15408-3-2017. Оценочный уровень доверия – уровень 5.

DLP помогает государственным органам выполнять нормативные требования и отраслевые стандарты соответствия информационной безопасности. Это помогает избежать юридических и финансовых последствий, возникающих в результате несоблюдения требований.

Имея возможность предоставляя оповещения в режиме реального времени и автоматизированные действия, DLP-системы помогают предотвратить утечку данных оперативно.

DLP-система позволяет получить информацию о хранении документов для служебного использования в памяти ПК и съемных носителях, быстро идентифицировать источник нарушения и предпринять соответствующие действия для локализации и устранения инцидента.

Внедрение DLP-системы способствуют формированию культуры безопасности данных в организации.

Также один из преимуществ DLP-системы это интеграция со СКУД системами.

С помощью vpn канала есть возможность осуществлять контроль рабочего времени сотрудников, вышедших на удаленный формат работы.

Слабые стороны.

Хоть и DLP-система обладает многочисленными преимуществами, у них также есть некоторые ограничения и потенциальные слабые стороны. К примеру, ложноположительные и отрицательные результаты: системы DLP могут генерировать ложноположительные и ложноотрицательные результаты, что влияет на их точность и эффективность. Ложные срабатывания возникают, когда законные действия помечаются как потенциальные нарушения, что приводит к ненужным предупреждениям и сбоям в работе.

Внедрение и настройка DLP-систем могут быть сложными и отнимать много времени. Они требуют глубокого понимания структуры данных государственного органа, политик и требований к безопасности. Настройка правил и политик DLP в соответствии с конкретными бизнес-процессами и информационными потоками требует специальных знаний и постоянного технического обслуживания.

DLP-системы могут испытывать трудности с проверкой зашифрованного контента, что ограничивает их способность обнаруживать потенциальные утечки данных или нарушения политики в рамках зашифрованных сообщений.

Киберугрозы и методы атак продолжают быстро развиваться. Изощренные злоумышленники могут использовать передовые методы обхода систем DLP, такие как запутывание конфиденциальных данных, использование скрытых каналов связи или использование уязвимостей в самой реализации DLP. Системы DLP нуждаются в регулярных обновлениях и усовершенствованиях, чтобы идти в ногу с возникающими угрозами.

Развертывание и запуск систем DLP могут привести к дополнительным накладным расходам и повлиять на производительность системы.

Вместе с этим, DLP-система предполагает сбор и анализ конфиденциальных данных, что может вызвать опасения по поводу конфиденциальности. Необходимо внедрять надлежащие меры предосторожности для защиты частной жизни отдельных лиц и обеспечения соблюдения соответствующих правил защиты данных.

Возможности.

Технологические достижения могут привести к созданию более сложных DLP-решений с повышенной точностью, улучшенной обработкой шифрования и улучшенными возможностями интеграции.

Растущие требования не только к защите данных но и к созданию единого, общего центра управления: создает возможности для поставщиков систем DLP предлагать решения, которые помогают государственным учреждениям соответствовать в меняющимся мире.

Есть потенциал тиражирования опыта внедрения в региональных областях и управлениях.

Вместе с этим функции систем DLP возможно настроить на проведение оптимизации штатной численности государственного органа.

Угрозы.

Постоянный прогресс в области киберугроз и методов атак создает проблемы для систем DLP, требующих постоянных обновлений и усовершенствований, чтобы идти в ногу со временем.

DLP-системы сталкиваются с трудностями при проведении различия между законным доступом и вредоносными действиями авторизованных пользователей, что затрудняет эффективное обнаружение внутренних угроз.

Проблемы конфиденциальности: сбор и анализ конфиденциальных данных с помощью DLP-систем вызывают проблемы конфиденциальности, требующие строгих гарантий конфиденциальности и соблюдения соответствующих нормативных актов.

Основные эффекты от внедрения систем DLP

Социальный эффект:

- предупреждение утечки конфиденциальной информации;
- повышение эффективности труда, в среднем, на 30%;

- противодействие коррупции посредством выявления деструктивных сотрудников.

Экономический эффект:

- импортозамещение, использование казахстанского DLP-комплекса;
- экономия бюджета при использовании одного программного комплекса вместо нескольких платных инструментов;
- предотвращение финансовых и репутационных рисков.

Регуляторный эффект:

- контроль качества обеспечения информационной безопасности;
- внедрение ПО, соответствующего законодательным требованиям;
- соответствие концепции «Киберщит Казахстана».

Операционный эффект:

- автоматизация рабочих процессов;
- контроль сотрудников на удаленной работе;
- централизация входящей и исходящей информации внутри организации.

Изучив теоретические и технические аспекты внедрения DLP-систем, структурируем в таблице 7 основные проблемы внедрения на государственной службе для разработки дальнейших рекомендаций.

Таблица 7 − Проблемы внедрения DLP-систем

№	Проблема	Пути решения/ для работы при внедрении
1	Сопротивление сотрудников	Разработать проект медиа-плана по разъяснению вопросов внедрения DLP-системы. *(Проект 1)*
2	Коммерческое предложение от поставщиков в условиях масштабирования опыта	К статьям расходов будет относиться не только сам продукт, а его лицензия, стоимость развертывания системы, техническая поддержка, интеграционные работы и ежегодное обновление.
3	Доступ к базе DLP	Подписание соглашения о неразглашении сведений частной жизни, личной и семейной тайны сотрудников. *(Проект 2)* Предусмотреть в служебных обязанностях сотрудников ДКР пункт по использованию DLP-системы для проведения служебных расследований.
Примечание – составлено автором		

Представленные проекты **Медиа-плана** и **Соглашение о неразглашении сведений** будет способствовать повышению доверия со стороны сотрудников, появится понимание внедрения проекта DLP и снизит сопротивление установки агентов на служебные компьютеры.

Соглашение создаст ответственность, при работе с получаемой и обрабатываемой информации от DLP-системы.

Потенциал интеграции DLP-системы со СКУД через API

Рассмотрим предложение экспертов по проведению односторонней интеграцией с Системой контроля и учета допуска на рис. 11.

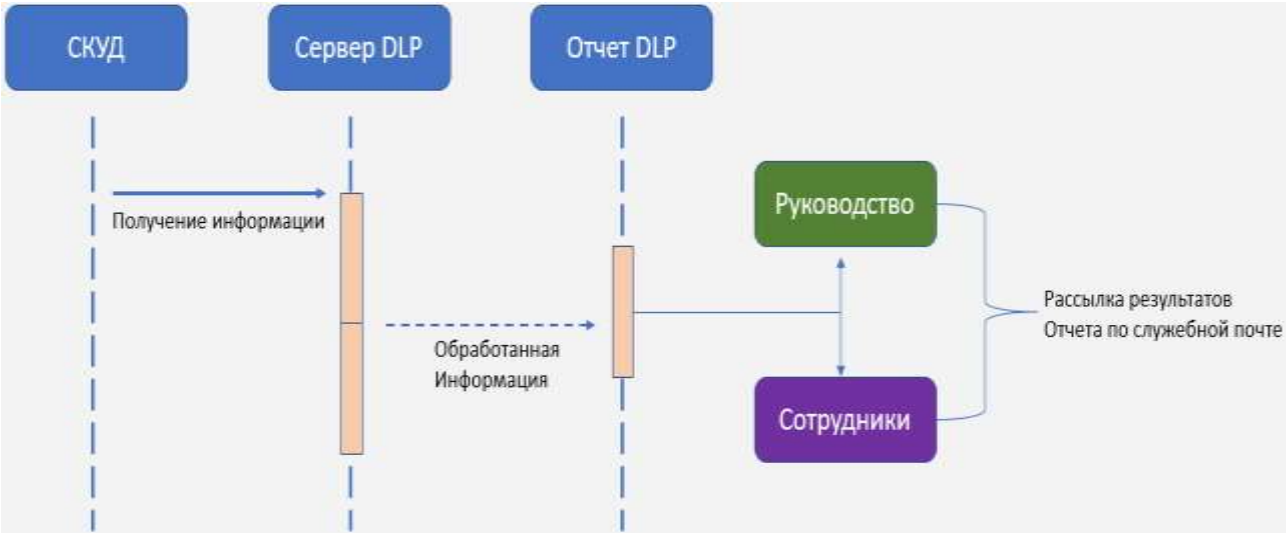

Рисунок 11 – схема интеграции DLP-системы со СКУД.
Примечание - составлено автором по результатам экспертного интервью

Система контроля и управления доступом — это совокупность программно-аппаратных технических средств контроля и средств управления, с целью ограничения и регистрации входа-выхода сотрудников организации

Основная функциональная задача — управление доступа в стратегически важный объект с идентификацией персоны, включая также ограничение доступа.

Имеющаяся система СКУД в МИИР может оповещать DLP о прибытии конкретного лица на рабочее место и уходе с него. Данную возможность можно использовать для повышения эффективности сотрудника путем контроля трудовой дисциплины и создания организационной культуры, а также, в случае если осуществляется рассылка сообщений от имени пользователя, и если через СКУД систему не регистрировался сотрудник, то в DLP-системе будет оповещен критически значимые инцидент, чем, когда пользователь находится на рабочем месте. Подключение такого источника данных потенциально важно для повышения эффективности сотрудников Министерства и обеспечения информационной безопасности.

К примеру, благодаря данной интеграции также возможно определить менее эффективных сотрудников, которые часто опаздывают на работу и нарушают трудовую дисциплину. Данные об этих сотрудниках будут автоматически формироваться в модуле «Отчеты» и рассылаться по служебной почте.

Стоит отметить, что по результатам социологического опроса 76,6% государственных служащих считают, что наиболее эффективный сотрудник тот, кто является ответственным.

Благодаря данной интеграции появится возможность повышать ответственность среди государственных служащих, что в целом положительно повлияет на начало эффективного рабочего дня.

Потенциал интеграции DLP-системы с АСП через API сервис

Рассмотрим проведению односторонней интеграцией с Автоматизированной системой пропусков на рис. 12.

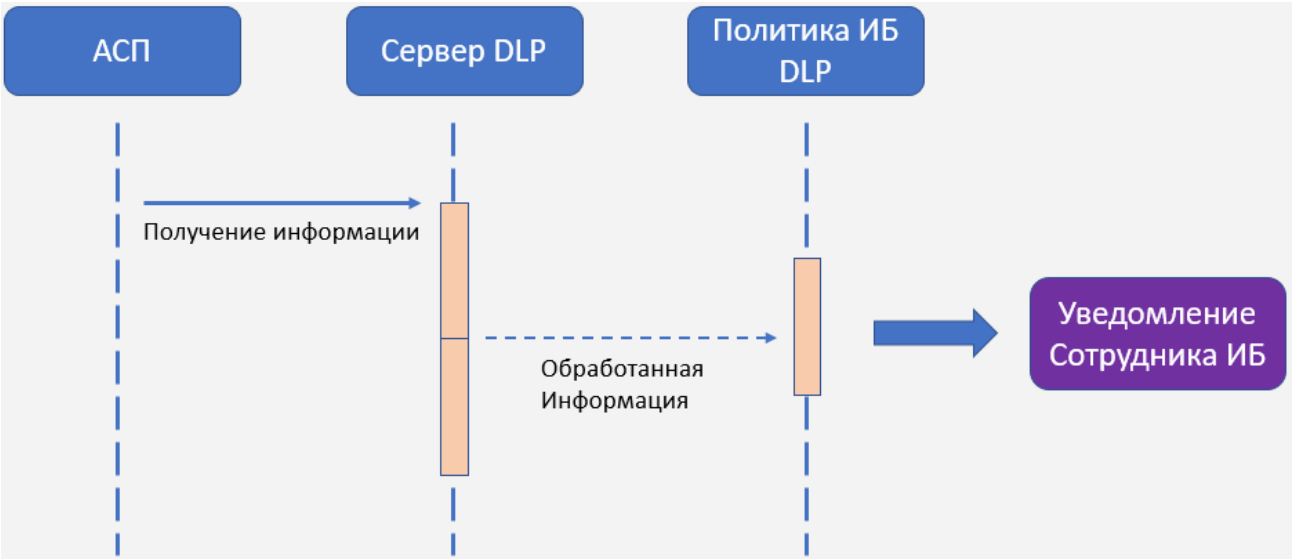

Рисунок 12 – схема интеграции DLP-системы с АСП.

Примечание - составлено автором по результатам экспертного интервью

Информационная система АСП предназначена для автоматического процесса заказа, согласования и оформления пропусков с ИНН в здание организации.

Имеющаяся система АСП в МИИР может оповещать DLP о прибытии гостей для надлежащего контроля конфиденциальной информации.

К примеру, возможность данной интеграции возможно использовать в целях предотвращения утечки секретных документов.

В случае, если гость вставит личный USB-флеш-накопитель то в DLP-системе будет оповещен критически значимые инцидент. Сотрудникам ИБ незамедлительно поступит уведомление о личности и моменте инцидента.

Подключение такого источника данных потенциально важно для повышения информационной безопасности.

Данная интеграция значительно повысит эффективность работы сотрудников информационной безопасности.

Возможность централизованного управления за инфраструктурой локальной сети и настройка политики безопасности облегчает исполнение функциональных обязанностей, затрачивается меньше времени.

Одно из преимуществ Казахстанского DLP комплекса, это готовый API сервис для проведения данной интеграции.

Потенциал интеграции DLP-системы с e-kyzmet посредством API сервисов

Рассмотрим проведению двухсторонней интеграции с системой e-kyzmet на рис. 13.

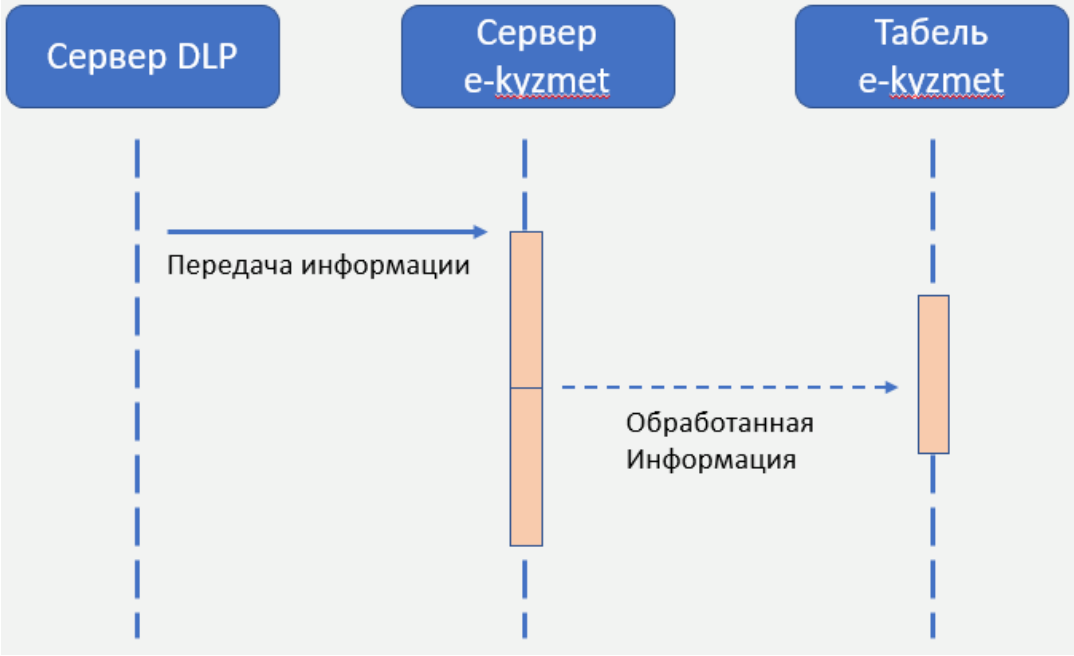

Рисунок 13 – схема интеграции DLP-системы с е-кызмет.
Примечание - составлено автором по результатам экспертного интервью

E-kyzmet является технологической базой электронного делопроизводства и предназначена для усовершенствования бизнес-процессов в системе управления персоналом государственной службы.

Благодаря данной интеграции появится возможность формирования автоматического табеля сотрудников подразделений. Что обеспечить прозрачность и открытость работы на государственной службе. В том числе выявление теневых сотрудников.

Данная автоматизация исключит человеческий фактор при формировании табеля, что положительно повлияет не только на эффективность работы

государственных служащих, но и на систему государственного управления в целом.

Основные рекомендации по использованию DLP-системы

Итак, изучив DLP систему и для решения поставленной цели проекта предлагается следующий перечень рекомендаций государственным структурам:

1. Перед внедрением DLP-систем утвердить проект медиа-плана и соглашения по разъяснению вопросов и масштабирования данной системы; *(см. проект 1,2)*
2. Предусмотреть при внедрении DLP-системы интеграционные работы с системами СКУД, АСП, е-кызмет; *(см. рис. 11,12,13)*
3. Использовать модуль «Политики безопасности» DLP-системы для отключения компьютеров по окончанию рабочего дня; *(см. таб. 3)*
4. Использовать модуль «Отчеты» DLP-системы для повышения эффективности работы сотрудников; *(см. таб. 2)*
5. Службам управления персоналом использовать модуль «Расследования» DLP-системы при проведении служебных расследований и принятии мер дисциплинарного характера.

Применение вышеуказанных рекомендаций полностью обосновано и практико-применимо на государственной службе. Подробной описание отражено в аналитической записке.

Заключение

Для внедрения DLP-системы с целью повышения эффективности деятельности государственных служащих выполнены такие задачи как, изучение теоретических и технических аспектов DLP-системы в государственном управлении. Проанализирован международный опыт передовых стран как США, Великобритания, Германия, Сингапур и т.д.

Через SWOT-анализ выявлены проблемы внедрения DLP-системы и представлены их пути решения по снижению уровня сопротивления сотрудников, масштабирование опыта, доступа к базе и информации.

В рамках исследования определены модули DLP-системы для возможности повышения эффективности государственных служащих.

Руководители департаментов могут использовать отчеты из выгрузки DLP-системы для контроля эффективной работы и совершенствования организационной культуры. Именно трудовая атмосфера в большей степени повлияет на эффективность работы сотрудников.

По результатам экспертного опроса наблюдается шаблонный метод мотивации сотрудников. Малое внимание уделяется организационное культуре, к примеру, сегодняшними руководителями государственных органов редко применяется поощрение за конструктивную обратную связь. Редко признаются индивидуальные и совместные усилия воспринимая их по долгу службы. Руководителям новой формации необходимо поощрять культуру непрерывного обучения и профессионального развития. Предоставлять возможности для обучения, повышения квалификации и обмена знаниями. К примеру, прикомандировать в общественные институты развития, которые находятся в структурном подчинении. Создавайте среду, в которой поощряются эксперименты и извлечение уроков из неудач.

Надо признать важность баланса между работой и личной жизнью. Поощрять культуру поддержки и заботливости в команде. Признавать заслуги сотрудника при собрании коллектива. А модуль отчетности DLP-системы послужит цифровым инструментом.

Повышение эффективности работы государственных служащих является важнейшей целью правительств во всем мире. Благодаря обширному обзору литературы и международного опыта становится очевидным, что различные стратегии и инициативы могут способствовать повышению эффективности работы государственных служащих. Эти усилия необходимы для обеспечения эффективного предоставления государственных услуг, совершенствования управления и содействия экономическому развитию.

Внедрение цифровых технологий, таких как системы предотвращения потери данных (DLP), стало многообещающим подходом к повышению эффективности. DLP-системы предоставляют инструменты и механизмы для защиты конфиденциальной информации, оптимизации процессов и повышения производительности. Международный опыт продемонстрировал эффективность систем DLP в государственных учреждениях, что приводит к повышению

безопасности данных, снижению рисков утечки информации и повышению операционной эффективности.

Однако внедрение DLP-систем также сопряжено с этическими проблемами. Контроль и отслеживание деятельности сотрудников с помощью DLP-систем вызывают опасения, связанные с конфиденциальностью, доверием и возможностью злоупотреблений. Поэтому крайне важно разработать соответствующие руководящие принципы, политику и гарантии для решения этих этических проблем, обеспечивая баланс между эффективностью и уважением прав личности и неприкосновенности частной жизни.

Поэтому в рамках магистерского проекта разработан проект Медиа-плана для профилактической и разъяснительной работы среди государственных служащих. В заключение следует отметить, что внедрение DLP-систем обладает значительным потенциалом для повышения эффективности работы государственных служащих. Повышая безопасность данных, оптимизируя процессы и способствуя лучшему распределению ресурсов, системы DLP могут способствовать более эффективному предоставлению государственных услуг. Однако важно подходить к их внедрению с тщательным учетом этических последствий и необходимости прозрачной политики и гарантий. Решая эти проблемы, правительства могут создать благоприятную среду, которая максимизирует преимущества систем DLP при соблюдении принципов этического управления и уважении прав государственных служащих.Как показала ранняя практика, с 2018 года система автоматического отключения компьютеров в госорганах через программу shutdown оказалась неэффективной так как, работа ПК продлевается самими государственными служащими, и они не запрашивают разрешения со стороны руководства и не прикрепляют обоснование на продление рабочего дня. Обслуживающая компания АО «Национальные информационные технологии» запросило дополнительное финансирование на внесение изменения в функционал данной программы. [17]

Учитывая внедрение DLP-системы в рамках концепции «Киберщит» имеется предусмотренная техническая возможность отключать служебные ПК без дополнительных финансовых затрат. Данная мера положительно скажется на эффективности работы государственных служащих, путем адаптации сотрудников на принудительное отключение ПК, уходя от тенденции перерабатывать и задерживаться на рабочем месте.

Также, в рамках исследования полностью раскрыт DLP-модуль «Расследования». Переход на новый уровень проведения служебного расследования повысит качество проводимой дисциплинарной работы и обеспечит прозрачность расследования.

Вместе с этим, в магистерском проекте раскрыт операционный алгоритм внедрения DLP-системы, представлена диаграмма Ганта и этапы работ с временным интервалом которую можно использовать в практической плоскости государственной службы.

В заключении стало известно, какие качества на сегодня определяют эффективного сотрудника в государственном секторе. Повышая навыки

оперативной работы, умение принимать решения, ориентированность на достижение результата, умение сотрудничать и акцентируя внимание на высокую ответственность государственные служащие будут эффективно служить народу Казахстана.

Список использованных источников

1 Концепция новой модели государственной службы Республики Казахстан Указ Президента Республики Казахстан от 21 июля 2011 года №119 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/U1100000119 Дата обращения: 14.04.2023 г.

2 Выступление Главы государства Касым-Жомарта Токаева на расширенном заседании Правительства // URL: https://www.akorda.kz/ru/vystuplenie-glavy-gosudarstva-kasym-zhomarta-tokaeva-na-rasshirennom-zasedanii-pravitelstva-106582 Дата обращения: 14.04.2023 г.

3 Мелимов А.А. Этические проблемы внедрения DLP-систем в условиях контроля за деятельностью сотрудников // Информационная безопасность: современная теория и практика: Сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции, Омск, 2019. – С. 77-81. – EDN UGJPIK.

4 Дубровина, А. И. Применение DLP - систем в технологиях защиты информации / А. И. Дубровина // Modern Science. – 2021. – № 3-2. – С. 479-482. – EDN UZAAIG.

5 Гниденко, И. Г. Критерии выбора DLP-систем / И. Г. Гниденко, И. В. Егорова // Цифровые технологии обработки и защиты информации : Сборник научных статей / Под редакцией Е.В. Стельмашонок, И.Н. Васильевой. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2020. – С. 59-64. – EDN CJULYG.

6 Кащеева, М. А. Исследование функционирования DLP-систем в коммерческих и государственных организациях / М. А. Кащеева, Л. М. Анищенко // Сборник избранных тезисов работ лауреатов II (2) Зимней научной сессии СНО НИЯУ МИФИ : Материалы II Зимней научной сессии СНО НИЯУ МИФИ, Москва, 13–19 декабря 2022 года. – Москва: Национальный исследовательский ядерный университет "МИФИ", 2022. – С. 48-49. – EDN FAGOHE.

7 Бекмурзиева Х.М. Мотивация деятельности государственных служащих как средство повышения эффективности государственной гражданской службы // Государственное и муниципальное управление. – Москва, 2018. – № 4(22) – С. 4-9.

8 Адаменко А.А. Повышение эффективности управления персоналом в структурах государственного управления // Вестник Академии знаний. – Москва, 2020. – № 40(5) – С. 12-17.

9 Скидан А.В., Чипига Ю.А., Исюк А.А. Цифровизация как фактор повышения результативности государственного управления: Проблемы и направления развития // Проблемы управления. – Москва, 2021. – № 10.22394/2079-1690 – С. 71-76.

10 Бирюкова Э. Р. Понятие «эффективность» в сфере государственного управления // Юридические науки. – 2020. – № 1. – С. 419-422.

11 Системные требования DLP // URL: https://faq.cyberguard.kz/d/5-kakovy-sistemnye-trebovaniya-dlp-kiberstrazh Дата обращения: 15.04.2023 г.
12 Как Минобороны США использует блокчейн для защиты данных // URL: https://novator.io/blokchejn/kak-minoborony-ssha-ispolzuet-blokchejn-dlya-zashhity-dannyh Дата обращения: 15.04.2023 г.
13 Национальная программа информационной безопасности Великобритании // URL:https://www.tadviser.ru/index.php Дата обращения: 15.04.2023 г.
14 Австралийское управление сигналов - Australian Signals Directorate // URL: https://ru.mgwiki.top/wiki/Australian_Signals_Directorate Дата обращения: 15.04.2023 г.
15 Сингапур запускает новую стратегию по обеспечению кибербезопасности // URL: https://internationalwealth.info/office/singapore-launches-new-cybersecurity-strategy/ Дата обращения: 15.04.2023 г.
16 ЕС принял новую Директиву о кибербезопасности // URL: https://www.infowatch.ru/analytics/novosti-ib/es-prinyal-novuyu-direktivu-o-kiberbezopasnosti Дата обращения: 15.04.2023 г.
17 Система автоматического отключения компьютеров в госорганах оказалась неэффективной// URL: https://informburo.kz/novosti/sistema-avtomaticheskogo-otklyucheniya-kompyuterov-v-gosorganah-okazalas-neeffektivnoy.html Дата обращения: 15.04.2023 г.

Аналитическая записка по результатам работы

Автор проекта: Абилов А.М.
Научный руководитель: Медебаева А.Б.

Идея проекта	Внедрение DLP-системы для повышения эффективности деятельности государственных служащих
Проблемная ситуация (кейс)	Совершенствование системы государственной службы путем внедрения новых технологий
Имеющиеся решения данной проблемы	DLP-система Преимущества: 1. Мониторинг за физическим состоянием сотрудников; 2. Проведение служебных расследований; 3. Отключение ПК по завершению рабочего дня; 4. Гибкость для проведения интеграционных работ с существующими ИС. Недостатки: 1. Доступ к личным данным сотрудников.
Предлагаемое решение данной проблемы	Для максимизации эффективности государственных служащих через DLP-систему предлагается: 1. Отключать ПК после 18:30; 2. Автоматическая выгрузка и рассылка по почте руководителям структурных подразделений; “Отчет по временной активности сотрудников”; 3. Предоставить доступ к базе DLP сотрудникам кадровой службы; 4. Автоматическое формирование табеля сотрудника через е-кызмет путем проведения интеграционных работ с DLP, СКУД. **Возможности** Отключение ПК после 18:30 способствует снижению показателя переработки и задержки на работе. Сотрудники адаптируются не откладывать задачи и решать их более оперативно, тем самым у них появится время для личной жизни и саморазвития. Из отчета DLP-системы по включению и отключению служебных компьютеров выявляются сотрудники, которые опоздали на работу, переработали или вовсе покинули рабочее место раньше завершения рабочего

	дня. Получив данную информацию, руководитель сможет эффективно управлять трудовой дисциплиной в коллективе и изменить организационную культуру к лучшему морально-психологическому климату. Для эффективного проведения служебных расследований в DLP-системе имеется модуль “Расследования”. Основная возможность модуля это, формирования дела и быстрый поиск необходимой информации на служебных компьютерах у сотрудников. Далее, собрав необходимые сведения, сотрудник управления служебных расследований сможет истребовать более качественные объяснительные по фактам нарушения исполнительской или трудовой дисциплины. Благодаря интеграции появится возможность формирования автоматического табеля сотрудников подразделений. Что обеспечить прозрачность и открытость работы на государственной службе. В том числе выявление теневых сотрудников. Данная автоматизация исключит человеческий фактор при формировании табеля, что положительно повлияет не только на эффективность работы государственных служащих, но и на систему государственной службы в целом. Также, интеграция со СКУД возможно для повышения эффективности сотрудника. К примеру, благодаря данной интеграции возможно определить менее эффективных сотрудников, которые часто опаздывают на работу и нарушают трудовую дисциплину. Данные об этих сотрудниках будут автоматически формироваться в модуле DLP и е-кызмет и рассылаться по служебной почте.
Ожидаемый результат	Формирование детальных отчетов о рабочем дне сотрудника и оценка его продуктивности. Улучшение и становление трудовой дисциплины частью организационной культуры организации. Соответствие стандартам информационной безопасности. Автоматизация работы кадровых служб и внедрение элементов цифровизации при проведении служебных расследований.
Литература	Список: 1. Концепция новой модели государственной службы Республики Казахстан Указ Президента Республики Казахстан от 21 июля 2011 года №119 // Информационно-правовая система нормативных

	правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/U1100000119 Дата обращения: 14.04.2023 г. 2. Бекмурзиева Х.М. Мотивация деятельности государственных служащих как средство повышения эффективности государственной гражданской службы // Государственное и муниципальное управление. – Москва, 2018. – № 4(22) – С. 4-9. 3. Мелимов А.А. Этические проблемы внедрения DLP-систем в условиях контроля за деятельностью сотрудников // Информационная безопасность: современная теория и практика: Сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции, Омск, 2019. – С. 77-81. – EDN UGJPIK. 4. Скидан А.В., Чипига Ю.А., Исюк А.А. Цифровизация как фактор повышения результативности государственного управления: Проблемы и направления развития // Проблемы управления. – Москва, 2021. – № 10.22394/2079-1690 – С. 71-76. 5. Дубровина, А. И. Применение DLP - систем в технологиях защиты информации / А. И. Дубровина // Modern Science. – 2021. – № 3-2. – С. 479-482. – EDN UZAAIG. 6. Кащеева, М. А. Исследование функционирования DLP-систем в коммерческих и государственных организациях / М. А. Кащеева, Л. М. Анищенко // Сборник избранных тезисов работ лауреатов II (2) Зимней научной сессии СНО НИЯУ МИФИ : Материалы II Зимней научной сессии СНО НИЯУ МИФИ, Москва, 13–19 декабря 2022 года. – Москва: Национальный исследовательский ядерный университет "МИФИ", 2022. – С. 48-49. – EDN FAGOHE.

Проект 1

МЕДИА-ПЛАН
по освещению и разъяснению вопросов
внедрения DLP-системы

№	Наименование мероприятия	Итог	Срок	Испол.
1	Проведение совещания на уровне руководителя аппарата с участием первых руководителей	Протокол внедрения DLP	*Внутренний*	*По положению ГО*
2	Подготовка исчерпывающих материалов о системе DLP	Единая рассылка сотрудникам	*Внутренний*	*По положению ГО*
3	Семинар на тему «Совершенствование DLP-системы и его функциональных возможностей»	Сбор предложений	*Внутренний*	*По положению ГО*
4	Освещение в СМИ	Испол. стратег. задачи	*Внутренний*	*По положению ГО*
5	Публикация в соц.сетях и справочнике организации контакты тех.поддержки	Публикация	*Внутренний*	*По положению ГО*
Примечания – составлено автором				

Проект 2

Соглашение о неразглашении сведений частной жизни, личной и семейной тайны при использовании DLP – системы

г. _____ **«__ » _____ 20__ г.**

_____ (*должность Ф.И.О.),* действующего (ей) на основании _____ *(наименование акта),* №_____ от _____ 20__ г. ознакамливается и заключает настоящее Соглашение с государственным органом о конфиденциальности и неразглашении информации в соответствии с Законодательством РК (далее - Соглашение).

1. Общие положения

1.1. Для целей Соглашения используются следующие понятия:

1.1.1. Информация - сведения (сообщения, данные) о предметах, фактах, о лицах и событиях;

1.1.2. Документ - зафиксированная на различных носителях, в том числе фото-, аудио-, видео.

1.1.3. Нераскрытая информация - Информация, неизвестная Третьим лицам техническая, организационная или коммерческая Информация, в том числе интеллектуальная собственность;

1.1.4. Коммерческая тайна - Информация, определяемая и охраняемая Работодателем, свободный Доступ на законном основании к которой имеет ограниченный круг лиц, разглашение, получение, использование которой может нанести ущерб его интересам;

1.1.5. Персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, Персональные данные ограниченного доступа относятся к Конфиденциальной информации, за исключением случаев, когда необходимо их раскрытие в соответствии с законодательством с письменного согласия Работодателя (например, предоставление информации об аффилированных лицах и т.п.);

1.1.6. Конфиденциальная информация - все виды Информации, в том числе Нераскрытая информация, Коммерческая тайна, а также банковская, налоговая, нотариальная, врачебная, личная, адвокатская тайна, в отношении которой в соответствии с законодательством, Соглашением, внутренними актами Работодателя ограничен доступ (установлена конфиденциальность), то есть установлено обязательное для выполнения лицом (Работником), получившим Доступ (Допуск) к данной Информации, требование не передавать (не разглашать) такую Информацию Третьим лицам без письменного согласия Работодателя;

1.1.7. Конфиденциальный документ - Документ, содержащий Конфиденциальную информацию, или Документ, созданный на основании Конфиденциальной информации;

1.1.8. Доступ - возможность получения Конфиденциальной информации и ее использования для служебной необходимости;

1.1.9. Разглашение - действия (бездействие) Работника, в том числе передача, распространение, раскрытие, утечка, в результате которых Конфиденциальная информация, в

любой возможной форме (устной, письменной или иной форме, в том числе с использованием технических средств) становится известной Третьим лицам, без письменного согласия;

1.1.10. Защита - принятие правовых, организационных и технических мер, направленных на исключение неправомерного Разглашения, Доступа, уничтожения, изменения, копирования и иных неправомерных действий в отношении Конфиденциальной информации;

1.2. Работник, состоящий в трудовых отношениях с Работодателем, выполняющий работу, связанную с необходимостью Доступа к Конфиденциальной информации, подписывая настоящее Соглашение, добровольно принимает на себя следующие обязательства:

1.2.2. Не Разглашать Третьим лицам Конфиденциальную информацию, которая станет ему известной в связи с исполнением трудовых (должностных) обязанностей и (или) в течении и после завершения трудовых отношений;

1.2.3. Своевременное обнаружение и пресечение несанкционированного доступа к Конфиденциальной информации;

1.2.4. Постоянный контроль за обеспечением уровня защищенности Конфиденциальной информации;

1.2.5. Недопущение воздействия на технические средства обработки Конфиденциальной информации, в результате которого нарушается их функционирование;

1.3. К Конфиденциальной информации относятся:

1.3.1. (*указать необходимое*)

1.4. Документ, создаваемый Работником, подлежит отнесению к категории Конфиденциальных документов при наличии одного из следующих условий:

1.4.1. В документе содержится Конфиденциальная информация и (или) Документ подготовлен на основе Конфиденциальных документов (воспроизводимой из таких документов или содержащейся в таких документах Информации);

1.4.2. Несанкционированное Разглашение содержащейся в Документе Информации может нанести Убытки и (или) ущерб интересам государства и (или) создать угрозу их нанесения либо сопряжено с рисками;

1.5. Необходимость отнесения Документа к категории Конфиденциальных документов определяется Руководителями (заместителями руководителей) структурных подразделений, подписывающими, утверждающими Документ либо согласовывающими проект Документа. Предложение об отнесении Документа (его проекта) к категории Конфиденциальных документов направляется уполномоченному на принятие соответствующего решения (подписание, утверждение Документа) лицу служебной запиской (письмом).

2. Ответственность

2.1. Нарушение Работником условий Соглашения и (или) актов Работодателя, регламентирующих вопросы обращения и Защиты Конфиденциальной информации, не ставшее причиной и не повлекшее за собой Разглашения Конфиденциальной информации, является основанием для привлечения Работника к дисциплинарной ответственности в виде: замечания, выговора, строгого выговора.

2.2. Основанием для привлечения Работника к ответственности являются выявленные факты неправомерного использования и (или) Разглашения Конфиденциальной информации и (или) Убытки, причиненные Работодателю Работником в результате виновного противоправного поведения (действия или бездействия)

3. Заключительная часть

3.1. Действие Соглашения начинается со дня его подписания.

3.2. Содержание Соглашения не подлежит разглашению третьим лицам за исключением случаев, предусмотренных законодательством РК.

3.2. Приложения, дополнения, изменения, совершенные в порядке, регламентированном Соглашением, являются его неотъемлемой частью.

Подпись

Дата