МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Информационная безопасность от внутренних угроз
Специальность: 5В100200 – «Системы информационной безопасности»
Выполнил: Емберди Абылайхан Байсуанулы Группа СИБ-15-3
Научный руководитель: Алавердян Егисабет Церуновна

Консультанты:
по экономической части:
к.э.н., профессор Ахметбаева Ж.Т.
(ученая степень, звание, Ф.И.О)
(подпись) «4» июня 2019 г.

по безопасности жизнедеятельности:
д.т.н., ст. преп. Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О)
(подпись) «4» июня 2019 г.

по применению вычислительной техники:
к.т.н., доцент Сатимова Е.Т.
(ученая степень, звание, Ф.И.О)
(подпись) «____» _____2019 г.

Нормоконтролер:
ст. преподаватель Макарова Л.Т.
(ученая степень, звание, Ф.И.О)
(подпись) «7» июня 2019 г.

Рецензент:
_____
(ученая степень, звание, Ф.И.О)
_____ «_____» _____2019 г.
(подпись)

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра систем информационной безопасности

Специальность 5В100200 – «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Емберди Абылайхану Байсуанулы

Тема проекта Информационная безопасность от внутренних угроз

Утверждена приказом по университету №124 от «26» октября 2018 г.

Срок сдачи законченного проекта «30» мая 2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): в проекте было изучено множество существующих методов социальной инженерии. Предложена общая классификация угроз для организаций. Был разработан метод борьбы с социальной инженерией, описывающий теоретические аспекты социальной инженерии, методы, позволяющие воздействовать на работников организации и методы, которые сотрудники должны придерживаться для того, чтобы: уменьшить реализацию угрозы социальных инженеров.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект включает в себя 6 глав, разделенных на подглавы, каждая из которых освещает определенную тематику.

В первой главе дипломного проекта представлен портрет нарушителя информационной безопасности.

Во второй главе дипломного проекта представлены теоретические и методологические основы социального инжиниринга, а так же методики противодействия им.

В третей главе представлена организация работ с лог – данными

В четвертой главе проводится внутренний контроль сотрудников, работающих с конфиденциальной информацией

В пятой главе рассматриваются необходимые условия труда для безопасной жизнедеятельности

В шестой главе технико-экономическое обоснование, показывающее актуальность исследования

Основная рекомендуемая литература:

1) Алавердов А.Р. Управление кадровой безопасностью организации – М.: Маркет ДС, 2010.

2) Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: Учеб. пособие. – М.: ФОРУМ, 2009.

3) Скиба В., Курбатов В. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Издательство Питер, 2008.

4) Кузнецов М. В. Социальная инженерия и социальные хакеры : учеб.–метод. пособие. – СПб.: БХВ–Петербург, 2010.

5) Аманжолова К. Б., Алибаева С. А. Экономика предприятий телекоммуникаций: Учебное пособие. – Алматы: АИЭС, 2003.

Консультанты по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Безопасность жизнедеятельности	Бекбасаров Ш. Ш.	04.03-04.06	
Экономическая часть	Аренбаева К. Г.	04.03-04.06	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Угроза конфиденциальной информации	15.01. – 21.01.19	
Угроза от собственных сотрудников	21.01. – 31.01.19	
Теоретические и методологические – основы социального инжиниринга	4.02. – 11.02.19.	
Организация работы с документами	12.02. – 20.02.19	
Внутренний контроль циркуляции – и утечки конфиденциальной информа	25.02 – 20.03.19.	
Анализ условий труда	04.03 – 04.06.19	
Технико-экономическое обоснование	04.03 – 04.06.19.	

Дата выдачи задания «___» _____2018 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Сотимова Е.Т.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Емберді А.Б.)
(Подпись) (Ф.И.О)

АННОТАЦИЯ

В данном дипломном проекте было изучено множество существующих методов социальной инженерии. Предложена общая классификация угроз для организаций. Был разработан метод борьбы с социальной инженерией, описывающий теоретические аспекты социальной инженерии, методы, позволяющие воздействовать на работников организации и методы, которые сотрудники должны придерживаться для того, чтобы: уменьшить реализацию угрозы социальных инженеров.

АҢДАТПА

Бұл тезис жобасында әлеуметтік инженерияның көптеген қол жетімді әдістерін зерттелді. Ұйымдар үшін қауіптердің жалпы жіктелуі ұсынылды. Әлеуметтік инженерлермен жұмыс жасау әдісі әзірленді, әлеуметтік инженерлердің теориялық аспектілерін сипатталды.

ANNOTATION

In this thesis project was studied a lot of available methods of social engineering. A general classification of threats for organizations is proposed. A method of dealing with social engineers was developed, describing the theoretical aspects of social engineers.

Содержание

Введение

Внутренние ИТ – угрозы входят в число лидеров по киберугрозам, отодвигая на задний план традиционных лидеров таких как хакерские атаки и вирусы. Это связано с несколькими причинами. Первый это успехи производителей средств защиты от внешних угроз и распространение их продукций. Достижения в области биометрии и других систем аутентификации позволяют создать практичную и эффективную систему защиты, включая единую точку входа и контроль учетных записей пользователей. Вся концепция кибер безопасности состоит из, разделении на «санкционированные» и «несанкционированные» действия.

Решая проблему защиты периметра информационной системы извне, производители средств обороны информации проигнорировали то, что пользователь делает с «авторизованным» доступом. Производители программного и аппаратного обеспечения, увеличивают количество каналов, портов и протоколов, с помощью которых законный пользователь может похищать информацию. Беспроводные протоколы Bluetooth и WiFi, съемные носители (от стандартных флэш-карт до смартфонов), программы синхронизации мобильных телефонов позволяют легко передавать огромные объемы информации.

Если посмотреть на программные продукты в области кибер безопасности, то там нет продукта, способного контролировать внутренние угрозы, особенно утечку и искажение секретных данных. Большинство электронных утечек последних лет были обнаружены и устранены не инструментами информационной безопасности, а хорошими старыми способами ведения бизнеса – физическим отслеживанием сотрудников, работой персонала и тому подобное.

Теоретический и практический интерес заключается в том, что рассматриваемые и решаемые вопросы позволят всесторонне изучить теоретические и практические аспекты борьбы с угрозами безопасности информации со стороны своего персонала, путем улучшения защиты конфиденциальной информации.

Целью работы является рассмотрение уголовного законодательства и криминалистическая характеристика незаконного доступа к компьютерной информации.

С этой целью были определены следующие задачи:

- определить, что законодательство Республики Казахстан считает охраняемой законом информацией в сфере ИТ;
- выявить характеристики элементов социального инжиниринга;
- рассмотреть классификацию методов незаконного доступа и их характеристики;
- разработать методики противодействия социальной инженерии;
- осуществить полный внутренний контроль циркуляции и утечки конфиденциальной информации.

1 Сотрудники связанные с рисками информационной безопасности

1.1 Конфиденциальная информация и ее потенциальные угрозы

Наблюдаемая в последние десятилетия эволюция процесса компьютеризации общества породила новую глобальную проблему: безопасность информации. Целенаправленное или непреднамеренное воздействие на информационную сферу из внешних или внутренних источников может серьезно подорвать эти интересы и создать угрозы безопасности и риски. Практика показывает, что любые враждебные действия, направленные против интересов компании, начинаются с поиска данных из открытых источников.

Информация имеет такие свойства:

- аутентичность – позволяет распознать источник ее происхождения;
- конфиденциальность – свойство быть безопасной от незаконного ознакомления;
- целостность – защищенность от несанкционированного изменения или уничтожения;
- доступность – свойство информации, подлежащей защите от несанкционированной блокировки.

В зависимости от содержания секретная информация содержит всю секретную и конфиденциальную информацию. Правовой режим для сведений с ограниченным доступом направлен на защиту информации, утечка которой может представлять собой существенные убытки для организаций.

Конфиденциальная информация состоит в основном из данных и знаний, известных определенному кругу людей и представляющих большую ценность для них. Что касается доступа к ней, проводятся организационные, технологические, законодательные и меры по разграничению доступа. Разглашение или незаконное применение этой информации может привести к существенному ущербу для владельца, за который автор может быть привлечен к ответственности в соответствии с действующим законодательством.

Конфиденциальность понимается как предотвращение возможности использования информации лицами, которые к ней не причастны. [1]

Конфиденциальная информация применяется для защиты коммерческой тайны или клиентов, а также другие данные, раскрытие которых по той или иной причине нежелательно для конкретной организации. Другими словами, это любая информация, раскрытие которой может нанести вред владельцу, пользователю или сотрудникам.

С этих позиций категории близки к этой концепции:

- клиентская тайна – вид конфиденциальной информации, хранящейся в организации, раскрытие которой может нанести материальный или нематериальный ущерб ее клиентам или деловым партнерам;
- банковская тайна – конфиденциальная информация о финансово–коммерческой деятельности клиентов банка, банк которой является

уполномоченным представителем;

- коммерческая тайна – вид конфиденциальной информации, хранящейся в организации, раскрытие которой может нанести ей материальный или нематериальный ущерб, как субъекту хозяйствования.

Вся секретная информация является таковой в силу ее важности для физических или юридических лиц, групп или государства в целом. В то же время важность этого вида информации оправдывается тем фактом, что информация не известна широкому кругу людей и именно с этой позиций она имеет определенную ценность. Формы и виды конфиденциальной информации можно сгруппировать по разным направлениям (рисунок 1).

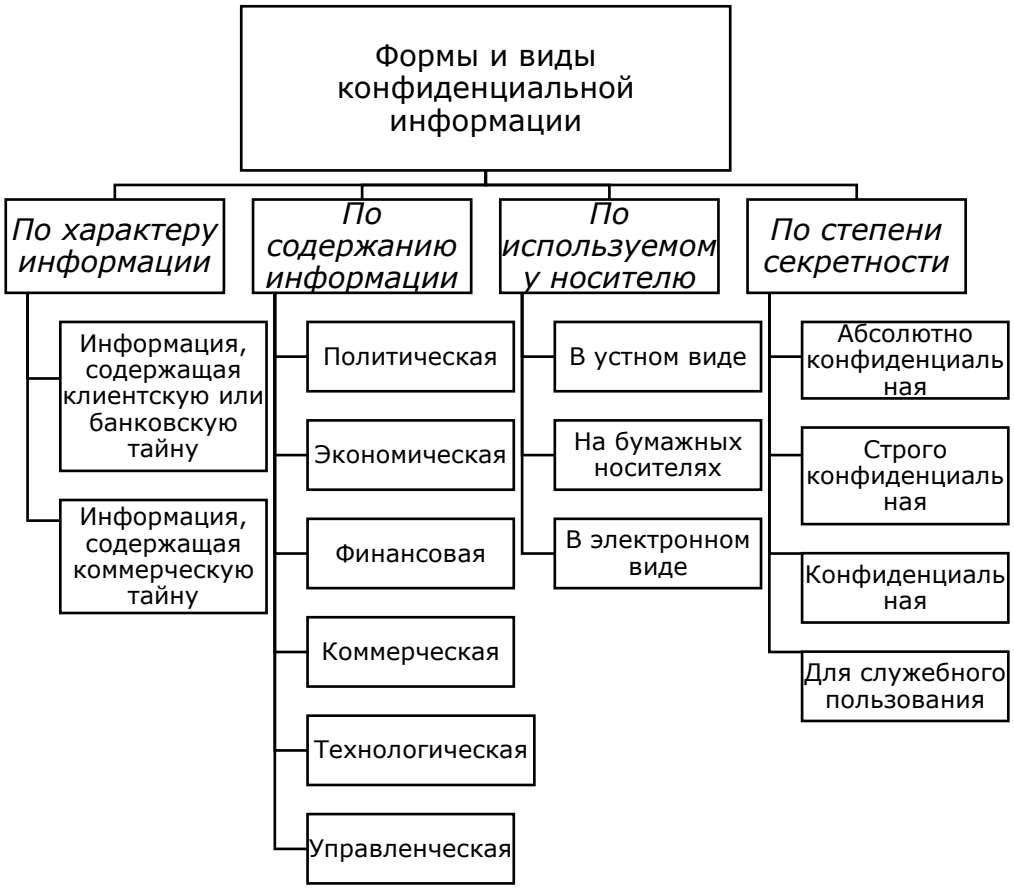


Рисунок 1 – Классификация конфиденциальной информации

В общем, конфиденциальную информацию можно символически поделить на три раздела:

- деловая информация предприятия или организации;
- информация, касающаяся непосредственно фактических данных о организации;
- ноухау – секреты производства.

Первая часть информации касается информации о деятельности предприятия или организации в определенной сфере, а именно: различные базы данных (клиентов, адресов, контрагентов), результаты исследований

статистического, маркетингового характера, конъюнктуры потребительского рынка и т.д.

Вторая часть информации затрагивает информации, характеризующей предприятие, такой как: сведения о банковских счетах, масштабах производства и договорах, заключаемых данным предприятием.

Третий блок информации можно обозначить как совокупность интелектуальных знаний, необходимых для организации.

Научно-технические разработки, экономические и организационные решения, неизвестные третьим сторонам, могут предложить предприятиям конкурентные преимущества и стать основным или дополнительным источником дохода. Передавая значительный объем информации в электронном виде, использование локальных и глобальных сетей создает новые качественные угрозы для конфиденциальной информации и конкурентной позиции организации в случае ее разглашения.

Помимо необходимости защиты производственных секретов организации, у информационной безопасности есть и другой аспект. Это связано с сохранением части конфиденциальной информации, раскрытие которой наносит ущерб интересам ее клиентов. Сюда входит любая информация о денежных средствах, финансовом состоянии партнеров и заемщиков, активах, переданных организации доверительного управления. Основным негативным последствием раскрытия этой информации является потеря репутации компании и имиджа в глазах партнеров и потенциальных клиентов. Организация, допустившая утечку информации, сразу теряет самых многообещающих партнеров среди корпоративных структур и крупных индивидуальных клиентов.

Невозможно создать эффективную систему защиты данных без четкого определения угроз для защищаемой информации. Угрозы информации обычно понимаются как потенциальные или фактические действия в отношении информационных ресурсов, приводящие к неправомерному владению информацией. Угрозы, связанные с доступом к секретным данным, можно сгруппировать по следующим признакам:

- по критериям кибер безопасности (угрозы конфиденциальности данных, программ, аппаратуры, угрозы доступности данных);
- по компонентам информационных систем, на которые нацелены угрозы (информационные ресурсы и услуги, персональные данные, ноухау);
- по методам реализации (случайные, умышленные, действия природного и техногенного характера);
- по месторасположению (внутренние и внешние).

Соответственно, можно выделить актуальные киберугрозы, которые направлены на снижение конкурентных позиций организации в случае ее разглашения:

- незаконное применение и поиск сведений;
- несоблюдение правил сохранности данных;
- ввод в ПО и техники компонентов, не соответствующих документам;

- рассылка вирусов;
- вывод из строя, уничтожение средств передачи информации;
- влияние наполитику парольных защит;
- утечка информации по техническим и физическим каналам;
- инсталяция жучков для перехвата информации;
- уничтожение или кража печатных и жестких дисков;
- перехват информации в сети и линии связи;
- распространение дезинформации, ведущее к потере репутации организации;
- эксплуатация не сертифицированных программ, антивирусов, телекоммуникации;
- неавторизованный доступ к базе данных.

Современный анализ ситуаций, связанных с доступом к конфиденциальной информации показывает, что финансовые корпорации и правительственные учреждения постоянно сталкиваются с внутренними угрозами в этой области.

Наиболее важными внутренними угрозами являются воздействия или же бездействие служащих, не соответствующие потребностям компании, которые имеют все шансы привести к экономическим убыткам компании, причинение ущерба репутации компании, появлению проблем с потенциальными клиентами и т. д.

Безопасность конфиденциальных данных на 80% связанно от принятия решения, ситуации, мотивации персонала. Большая часть внутренних угроз осуществляется с помощью персонала, поэтому основным источником таких угроз являются сотрудники этой организации. Поэтому риски и негативные угрозы, связанные с деятельностью персонала организации и, прежде всего, с деятельностью ее безответственных и недобросовестных сотрудников, требуют дальнейшего рассмотрения. [2]

1.2 Угрозы, от безответственных и нелояльных сотрудников

Человек всегда был уязвимой целью перед лицом угроз утечки и потери информации. Это свидетельствует о том, что проблема существования недобросовестных и безответственных работников очень болезненна для организации.

Чтобы лучше понять потенциал утечки информации и определить способы ее предотвращения, рекомендуется принять во внимание существующие классификации самих правонарушителей и классификацию угроз, связанных с персоналом. Таким образом, существует несколько разных классификаций внутренних нарушителей – организационных инсайдеров.

Халатные нарушители являются самым часто встречающимся видом внутренних нарушителей. Их нарушения в основном носят немотивированный характер и не имеют конкретных целей.

Нарушители, которыми манипулируют – это те сотрудники, которых обманным путем толкают на нарушение установленных норм. Такие сотрудники часто и не подозревают о том, что их действия приводят к потере конфиденциальных данных.

Обиженные нарушители (саботажники) – это сотрудники, которые стремятся нанести вред компании по личным причинам.

Сотрудники, которые занимаются продажей конфиденциальной информации и инсайдеры – это сотрудники, цель которых определяет заказчик хищения информации. В обоих случаях инсайдеры стремятся как можно надежнее спрятать свои действия. [6]

Подробнее рассмотрим внутренние и внешние угрозы кибер безопасности, связанные с персоналом.

Внешняя угроза рассматривается как угроза, источник которой находится за пределами компании. Внешние угрозы включают незаконную деятельность преступных организаций, конкурентов, компаний и частных лиц, вовлеченных в промышленный шпионаж и социальную инженерию. [3]

Внутренние угрозы включают в себя невнимание или преднамеренное действие со стороны персонала по раскрытию информации, а также мошенничество со стороны ведущих экспертов: «откаты», фальсификация документации компании с помощью оборудования и интернета, «необходимые» изменения в отчетных документах.

Рассмотрим эти угрозы более подробно:

а) внешний:

1) промышленный шпионаж. Под "промышленным шпионажем" подразумевается законное и незаконное извлечение информации конкурирующими компаниями. Научные исследования, производство наиболее перспективных технологий, а также персональные данные для использования в корыстных целях.

Промышленный шпионаж чаще всего направлен на: проверку надежности торгового партнера, уничтожение конкурента или причинение

ему серьезных убытков. И если в первом варианте нет прямой угрозы для организации, во втором случае, если конфиденциальная информация попадет в руки таких агентов, это может иметь очень серьезные последствия для компании, что приведет к банкротству и ликвидации.

В этом случае, используя технические средства, промышленные шпионы часто обращаются к сотрудникам компании за информацией. Даже сотрудники более низкого уровня могут установить соответствующее оборудование для удаления информации. Поэтому промышленный шпионаж является важной внешней угрозой, от которой нужно защищаться. Однако промышленные шпионы не достигли бы цели без внутренних угроз: безрассудных или преднамеренных действий своих сотрудников; [4]

2) социальная инженерия – незаконный метод подхода к базе данных без применения каких-либо электронных устройств. Полагается на использовании психологических аспектов человеческой натуры и считается очень разрушительной. Враг извлекает разнообразные сведения, с помощью мобильного звонка или путем входа в компанию под предлогом своей услуги.

б) внутренние:

1) неосторожность персонала. Очень часто сотрудники, хотя и не имеют целью разгласить конфиденциальные сведения, делают это. Поэтому неосторожность можно разделить на две категории: действия или бездействие сотрудников, вызванные неосведомленностью в сфере защиты информации.;

2) умышленные действия работников по разглашению информации. Целью действий сотрудников было именно разглашение информации, являющейся конфиденциальной. Причем сотрудников могли завербовать агенты промышленного шпионажа или же они сами инициативно решили предать организацию, на которую работали.

Что-бы свести к минимуму риски утечек руководству организации следует крайне серьезно и ответственно подходить к проблеме защиты конфиденциальных сведений от кибер-угроз. [5]

1.3 Способы защиты конфиденциальных данных

Чтобы нейтрализовать и минимизировать внутренние угрозы конфиденциальных сведений, необходимо предпринять следующие действия:

- организационные меры по защите информации;
- контрольно-правовые меры (выполнение персоналом инструкций, приказов, распоряжений, соответствующих нормативных документов);
- профилактические меры (предназначенные для мотивации персонала на полное соблюдение требований плана, правил работы, а также для создания соответствующего морального и этического состояния в команде);
- технические меры (шифрование, разграничение прав доступа);
- работа с персоналом (подбор персонала, брифинги, обучение персонала по вопросам информационной безопасности, повышение бдительности персонала, развитие навыков);
- психологические меры (установка видеонаблюдения, выявление

инцидентов с целью получения официальной информации вне организации).

Правовая основа кибер безопасности в организациях базируется на следующих регулирующих требований:

- Конституция Республики Казахстан;
- Гражданский кодекс Республики Казахстан;
- Трудовой кодекс Республики Казахстан;
- Уголовный кодекс Республики Казахстан;
- Закон от 24.11.15 «Об информатизации»;
- Указ от 14.11.11 «О концепции информационной безопасности Республика Казахстан»;
- Государственный стандарт ИСО/МЭК 17799–2006 Методы обеспечения защиты свод правил по управлению защиты информаций;
- Государственный стандарт ИСО/МЭК 27001–2008. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- Государственный стандарт ИСО/МЭК 27002–2009. Методы обеспечения защиты. Свод правил по управлению защитой информации;
- Государственный стандарт ГОСТ 50739–2006. Средства вычислительной техники. Защита от несанкционированного доступа к информации.

Общий надзор за соблюдение законодательства о персональных данных и их защите осуществляют органы прокуратуры.

За неисполнение законных требований предусмотрено наказание:

Статья 211 УК РК Неправомерное распространение электронных информационных ресурсов ограниченного доступа.

1) Незаконное распространение информационных ресурсов, содержащих персональные данные граждан, доступ к которым ограничен законами или их владельцем, наказывается штрафом в размере 200 МРП либо привлечением к общественным работам на срок до 180 часов, либо арестом на срок до 50 суток, с заниматься определенной деятельностью на срок до 3 лет.

2) То же деяние, совершенное: группой лиц по предварительному сговору, из корыстных побуждений, лицом с использованием своего служебного положения, наказывается привлечением к общественным работам на срок до 1200 часов либо ограничением свободы на срок до 5 лет.

3) Деяния, предусмотренные частями первой или второй этой статьи: совершенные преступной группой, повлекшие тяжелые последствия, наказываются лишением свободы на срок от 3 до 7 лет с лишением права заниматься определенной деятельностью.

Статья 369 УК РК Халатность.

1) Халатность, т.е. ненадлежащее исполнение лицом, занимающим ответственную государственную должность, своих обязанностей, если это повлекло причинение вреда правам и законным интересам граждан или организаций - наказывается штрафом в размере до 1000 МРП либо

исправительными работами в том же размере, либо лишением свободы на срок до года.

2) Те же деяния, повлекшие по неосторожности тяжелые последствия, - наказываются лишением свободы на срок до 5 лет с лишением права заниматься определенной деятельностью.

Статья 79 АК РК Нарушение законодательства о персональных данных и их защите:

1) Незаконная обработка, сбор персональных данных влечет штраф на физических лиц в размере от 20 до 100 МРП, с конфискацией предметов и орудия административного правонарушения.

2) Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, влекут штраф от 50 до 200 МРП, с конфискацией предметов и орудия административного правонарушения.

3) Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных влечет штраф от 100 до 300 МРП.

4) Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, влечет штраф от 200 до 1000 МРП.

Статья 185 АК РК Нарушение обязанности сохранения коммерческой, банковской тайны, сведений кредитных отчетов или информации из базы данных кредитных историй кредитного бюро.

1) Нарушение обязанности сохранения сведений, содержащих коммерческую, банковскую тайну, сведений кредитных отчетов или информации, полученных из базы данных кредитных историй, без согласия их владельца лицом, которому они стали известны в связи с профессиональной деятельностью, если это действие не содержит признаков уголовно наказуемого деяния, влечет штраф в размере 50 МРП. [7]

Организационно правовые методы защиты информации заключаются в ограничении доступа посторонних лиц и работников организации к объектам, содержащим секретную или конфиденциальную информацию. Основное назначение этих методов защиты – не допустить неправомерные действия. Атака такого типа может выполняться как пассивным (чтение секретной информации), так и активным (изменением информации) способом.

Помимо использования юридических и организационных методов для предотвращения несанкционированного доступа, необходимо установить физические барьеры.

Чтобы предотвратить утечку голосовой информации по виброакустическим каналам, предпринимаются шаги для определения каналов утечки. В большинстве случаев при несанкционированном удалении информации в комнате злоумышленник использует соответствующие технические устройства.

Технические способы обороны можно разделить на:

– средства аппаратной защиты, включающие средства защиты сети, систем электропитания;

– ПО защиты, в том числе: шифрование, антивирусы, системы разграничения и контроля доступа и т.п.

Внутренняя система информации и документооборота является наиболее уязвимой для сотрудников компании. Доказано, что 80% всех информационных потерь или искажений являются результатом злонамеренных действий, совершенных сотрудниками компании. Единственный способ избежать этого – соответствующая кадровая политика организации, которая направлена на повышение заинтересованности сотрудников в успешной работе путем развития чувства ответственности за свою работу. Следует рассмотреть порядок реализации каждой из функций управления персоналом для обеспечения кибер безопасности.

Подбор персонала. При приеме на работу провести тщательный опрос, чтобы узнать уровень интеллекта, чтобы иметь общее представление о кандидате как личности, определить морально-психологический уровень, криминальные наклонности. Конкретная работа нового сотрудника, должна начинаться со стажировки, по окончании которой принимается решение о приеме кандидата на постоянную работу. В случае успеха проверки и признания кандидата, его соответствующей должности, производится заключение двух документов:

1) трудового договора;

2) обязательства о неразглашении конфиденциальных данных.

Организация персонала предполагает обучение сотрудников правилам и методам работы с конфиденциальной информацией.

Внутреннее методическое содержание учебной программы должно включать:

- общие правила обеспечения безопасности организации с обязанностью работника соблюдать установленные правила;
- перечень полномочий службы безопасности по контролю и непосредственному функциональному управлению соответствующей деятельностью персонала;
- рекомендации по предотвращению ситуаций, которые могут повлечь за собой то что работник будет принят на работу и шантажирован;
- поведенческие рекомендации в случае вербовки и шантажа.

Как правило, обучение новых сотрудников осуществляется руководителями структурных подразделений. Целью данного тренинга является ознакомление с правилами обеспечения безопасности на определенных рабочих местах в рамках их обязанностей. Организация непрерывного обучения сотрудников осуществляется службой безопасности в режиме профессионального развития персонала. Соответствующие формы обучения можно дифференцировать следующим образом:

- для высшего руководства – это специальные информационно аналитические журналы, разосланные ежеквартально и подписанные

начальником службы безопасности;

- для остальных сотрудников – специальный брифинг, организованный не реже одного раза в шесть месяцев одним из специалистов служб безопасности.

Мотивация сотрудников организации к обеспечению безопасности их информации может быть реализована двумя способами: с помощью стимулов и санкций. Специальные стимулы (бонусы) для активной работы по повышению кибер-безопасности компании могут быть использованы для:

- ИТ и другой обслуживающий персонал, который разработал новые программные средства для повышения уровня защиты баз данных и коммуникаций;
- сотрудники службы безопасности, которые выявили источники утечки конфиденциальной информации, разработали новые технологии или методы защиты информации в устной и бумажной форме и успешно внедрили особо важные оперативные меры для противодействия реальным угрозам безопасность информации;
- руководители служб, в отношении которых службы безопасности не комментировали в отчетном году соблюдение правил безопасности информации.

Штрафы в отношении сотрудников и отдельных рабочих групп за нарушения, совершенные ими в области кибер безопасности, применяются при предоставлении услуги безопасности или ответственность за эти команды. По характеру контрольных действий они делятся на три группы:

1) административные санкции, наиболее серьезные с точки зрения воздействия (например, отзыв мандата, отказ от продления трудового договора, перевод работника на другое рабочее место, исключение работника из резерва назначения и т. д.);

2) экономические санкции (включая: лишение или уменьшение переменной части заработной платы при использовании таких базовых схем заработной платы, лишение или уменьшение ежеквартального бонуса для конкретного сотрудника или всех структурных подразделений команды и т. д.);

3) санкции психологического характера (например, индивидуальный разговор с менеджером или представителем отдела безопасности компании, обсуждение нарушения, совершенного сотрудником на заседании подразделения и т. д.). [7]

Субъектами контроля являются: начальники отделов, специалисты по безопасности, эксперты из частных агентств приглашенных для проведения внутренних расследований. Объектами управления являются два аспекта деятельности сотрудников организации:

- их соответствие правилам политик безопасности;
- лояльность к организации и начальству.

Таким образом, для организаций, обеспокоенных долгосрочными перспективами развития, важно сохранить персонал. Лояльность персонала

считается универсальным компонентом безопасности сотрудников, поскольку отношение сотрудника к своей организации усиливает или разрушает систему кибер безопасности. Сотрудники, которые лояльно относятся к компании, гораздо более устойчивы к сотрудничеству с конкурентами, мошенничеству и злоупотреблению властью. Лояльные сотрудники критикуют коллег, которые нарушают правила организации, предотвращая внутренние угрозы. [8]

Краткие выводы по главе

Таким образом, изучение теоретических аспектов, связанных с недобросовестными и безответственными работниками организации как субъектами кибер-угроз работодателя, проведено в рамках первой главы данной дипломной работы, сделаны следующие выводы:

1) в развивающейся рыночной экономике информация становится ценным активом. Поэтому основной задачей компаний является защита конфиденциальной информации, которая позволяет организации гарантировать экономическую безопасность, избежать банкротства, защитить себя от конкуренции, предотвратить атаки инсайдеров;

2) действия или бездействие (преднамеренное или непреднамеренное) работников, которые противоречат интересам компании, являются основными внутренними угрозами безопасности информации компании. Эти действия могут нанести экономический ущерб бизнесу, потерю информационных ресурсов, нанести ущерб имиджу компании, проблемы с реальными или потенциальными партнерами. Игнорирование угроз конфиденциальности информации может привести к серьезным потерям и убыткам для организации. Это не только финансовые проблемы, но и ущерб репутации;

3) для нейтрализации и сведения к минимуму внутренних угроз для конфиденциальной информации, исходящих от собственного персонала нужно применять в комплексе: организационные меры защиты информации, правовые меры, инженерно-технические мероприятия, кадровые и психологические ресурсы;

4) важнейшим элементом этого комплекса является кадровая политика организации, а именно:

- кадровое планирование (более тщательный отбор, опрос и проверка потенциальных сотрудников);
- организация персонала (внутреннее обучение, направленное на консолидацию общих правил безопасности и развитие навыков, необходимых для противодействия попыткам вербовки и шантажа);
- мотивация (применение соответствующих стимулов и санкций);
- контроль (постоянный мониторинг соблюдения сотрудниками информационной безопасности и оценка уровня лояльности).

2 Методологические принципы социальной инженерии

2.1 Цели социального инжиниринга

Социальная инжинерия – это способ незаконного доступа к информации или базам данных без использования специального оборудования. Основная цель социальных инженеров – получить доступ к защищенным системам для кражи секретных данных. Отличие от проникновения заключается в том, что в роли атакующего объекта выбирается не компьютер, а человек. Следовательно все средства и способы основаны на использовании слабостей человеческого характера, что считается чрезвычайно рисковано, поскольку злоумышленник получает информацию с помощью мобильного телефона или входа в организацию под видом коллеги.

Концепция «социальная инженерия» появилась относительно недавно. Суть социальной инженерии состоит в том, чтобы заставить особу сделать что-то плохое, но нужное для социального инженера. [9]

Социальная инженерия сформировалась как отдельная часть психологии. В основном все способы социальной инженерии основаны на когнитивной базе человека то бишь принятие решения.

Разговорить человека, чтобы тот выдал все сведения или просто заставить что-то сделать, считается пиком мастерства. Специалисты в данной сфере посредством интонации могут определять психологические склонности и фобий человека и моментально воспользоваться ими.

По сути социальная инженерия организованна на желании людей помочь другим. Социальная инженерия – самый эффективный инструмент в арсенале злоумышленников. Обычно использует вымысел, авторитет и уговоры. Наиболее часто социальная инженерия применяется для извлечения тайн, имеющей огромную значимость. Главные области использования показаны на рисунке 2.

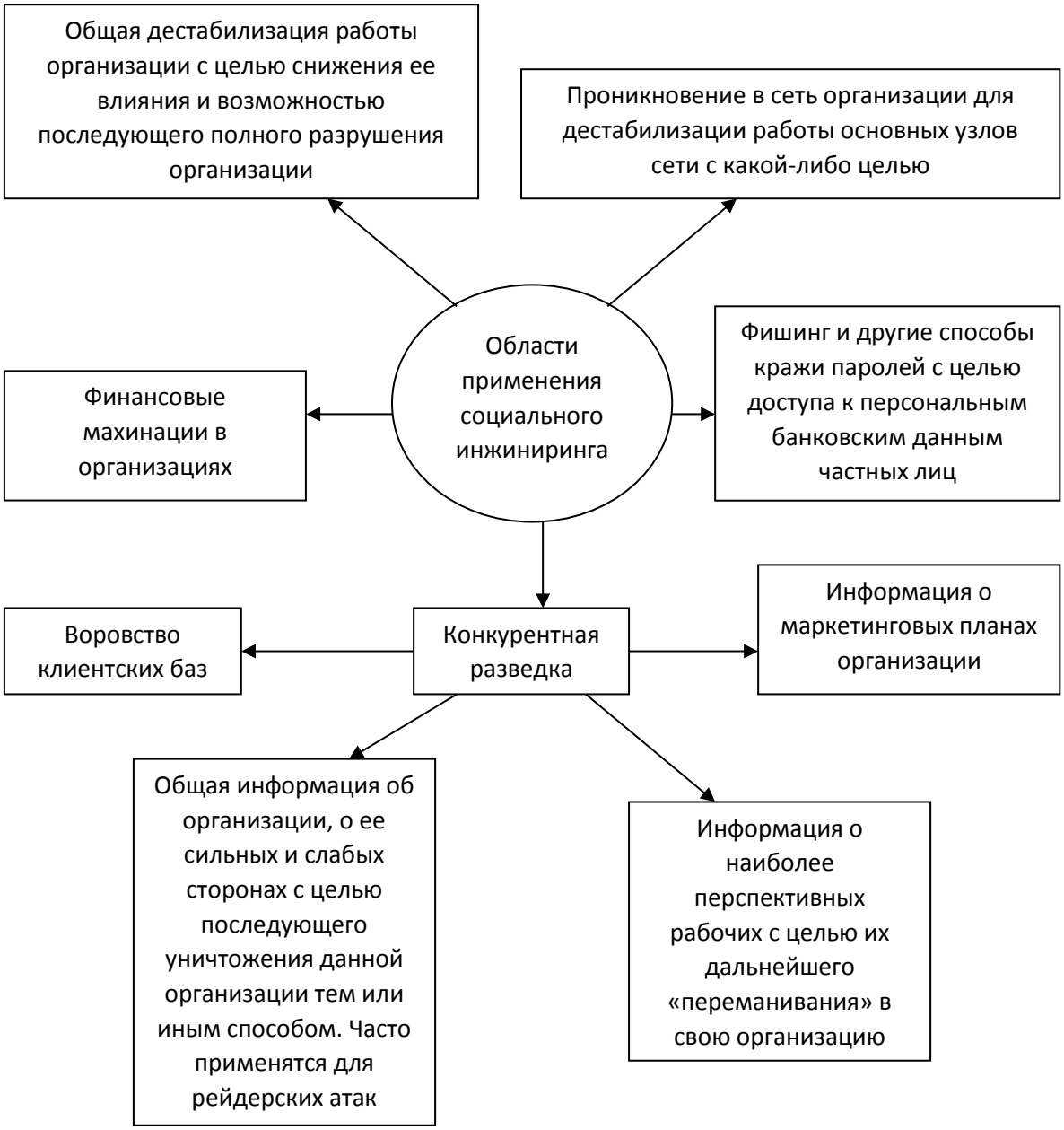


Рисунок 2 – Область использования социального инжиниринга

Основная масса инженеров социальных наук используют идентичные или схожие повадки. Поэтому изучение этих приемов позволяет распознать истину и не разглашать секретную данные.

Удачливые мошенники часто используют методы социальной инженерии и, манипулируют пользователями. Поэтому необходимо, чтобы компании уделяли достаточное внимание для этого важнейшего элемента безопасности.

Определение сути социальной инженерии ее разнообразий, таких как внушение и гипнотизирование – это связь между разумом и чувствами. С их помощью можно манипулировать людьми, как душе угодно.

Подготовка кибер-атаки делится на три этапа:

1) нахождение мишени (высчитывание и поиск необходимых сведений);

2) сбор всевозможной информации об объекте атаки;
3) порядок действий (проработка сценария до мелочей).

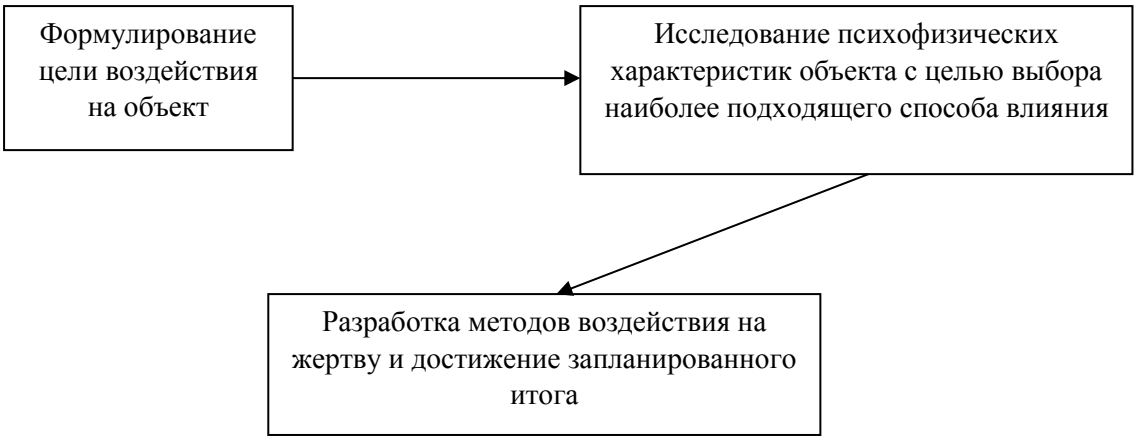


Рисунок 3 – План способов действий социальных инженеров

Социальный инжиниринг, в сочетании со знаниями систем кибер безопасности, пускают в ход для достижения этих целей:

1) комплектование всевозможных данных о жертве;
2) извлечение коммерческих тайн;
3) добыча сведений, необходимых для последующей авторизации;
4) принуждение жертвы сделать необходимые действия.

Атаки социальных инженеров представлены в виде рисунка 4.

Рисунок 4 – Схема воздействия в социальном инжиниринге

Сначала определяется суть давления на жертву. Далее собирается информация об объекте, после чего наступает этап аттракции. Аттракция - это моделирование комфортных условий. Принуждение к нужному для социального инженера итогу чаще всего получается выполнением предыдущих этапов.

Львиная часть информации компании не секретна, но она очень полезна для мошенника, поскольку она играет важную роль для повышения доверия. Иной раз знание внутренней терминологии может сыграть значимую роль.

Одним из основных методов является создание доверительных отношений с жертвой. Кибермошенник в основном выбирает сотрудника с невысоким знанием компьютерных технологий.

Главными виновниками успешных претворений социального инжиниринга являются:

1) страх;
2) любознательность;
3) меркантильность;
4) превосходство;
5) доверчивость. [8]

2.2 Методы и типы атак

Техники социальной инженерии:

1) претекстинг – это набор действий, выполняемых по предопределенному тексту. Этот метод реализуется с помощью мобильного или стационарного телефона. Во многих случаях этому методу необходимы хоть какие-нибудь сведения о человеке. Популярная стратегия с применением этого метода заключается в эксплуатации сначала незначительных вопросов и упоминании имен реальных коллег, в будущем кибер-мошенник говорит, что они нуждаются в помощи, и т.п. После установления дружественных отношений он может попросить о чем-то более существенном и важном;

2) фишинг – это тип кибер-мошенничества, целью которого является доступ к аутентификационным данным. Добивается успехов с помощью массовой отправки сообщений от лица брендов или в социальных сетях (Facebook, Вконтакте, Instagram). Письмо содержит ссылку на очень похожий фейковый сайт. Никакая крупная утечка личных данных не проходит без волны подобных рассылок. В настоящее время многие ссылки нацелены на кражу регистрационных данных и 65% из них успешны;

3) услуга за услугу – В основном социальный инженер говорит, что он из технической поддержки, который выявляет проблемы. В процессе решения принуждает жертву вводить нужные ему команды для устанановки вредоносного ПО;

4) троянский конь - этот метод использует человеческие эмоции. Открыв файл, прикрепленный к письму, запускается скрипт вируса удаленного доступа.

5) поиск сведений с социальных сетей. Например, "Твиттер", "Instagram", "ВКонтакте", содержат огромное количество данных нужных для злоумышленника;

6) дорожное яблоко – применяется вместе с физическими носителями. Социальный инженер бросает зараженный диск или флэш-карту в людном месте. Носитель сопровождается подписью (например, социальный инженер может запустить диск с ссылкой на официальный сайт организации, с

заголовком "заработная плата руководства". Сотрудник по незнанию и из любопытства вставляет его в компьютер);

7) Обратная социальная инженерия. То есть когда жертва сама предлагает злоумышленнику необходимые данные для быстрого решения проблем;

8) техническая социальная инженерия. В атаках этого типа используются общепринятые стереотипы такие как: " стоит камера, а значит ничего не украдут, и я в безопасности";

9) личный зрительный контакт - это самый сложный метод. Эту технику могут реализовать только профессиональные психологи или специально обученные люди. Т.е. чтобы человек сам все рассказал и не заметил этого;

10) анализ мусора – бумажные отходы бесценны, так как во время атаки она может помочь казаться сотрудником организации; [11]

2.3 Контрмеры против социальной инженерии

Чтобы защитить компании и персонал, нужно использовать многослойные интегрированные системы защищенности. Специфика этих систем следующие:

1) физическая безопасность – это ограничение путей к кабинетам, зданию и ресурсам компании;

2) любые сведения являются коммерческой тайной (счета, почтовая переписка и т.п.). При разработке мер защиты данных необходимо определить правила управления бумажными и электронными носителями информации;

3) компьютеры – защита программно-аппаратных частей;

4) локальная сеть – защита периметра сети, через которую взаимодействуют системы компании.

Сотрудникам надо напоминать, что в случае разглашения коммерческой тайны они будут наказаны и уволены в соответствии с соответствующими статьями УК и ТК РК, что в свою очередь окажет негативное последствие на дальнейшее трудоустройство.

Стоит поддерживать бдительных сотрудников, которые выявляют попытки атак, на конфиденциальные сведения. Очень важно, чтобы все члены организации, придерживались предопределенных правил при общении с пользователями и сотрудниками. Нужно научить сотрудников задавать вопросы для подтверждения личности, и говорить нет если это противоречит правилам.

Сотрудникам следует сообщать в службу технической поддержки, если с ними разговаривает лицо, выдающее себя за сотрудника тех поддержки. Сотрудники должны записать имя и фамилию абонента, номер телефона и наименование отдела, прежде чем положить трубку.

Так же необходимо:

- вести журнал всех действий, чтобы быстро исправить или ограничить возможные убытки в случае атаки;

- иметь четкие условия при обработке подозрительных запросов.

Аудит всех процедур является наиболее ценным средством для недопущения инцидентов и дальнейших расследований.

Кроме того, в документации следует отметить, что пользователям запрещено копировать ПО и данные, принадлежащие организации, забирать их домой или использовать их любым другим способом.

Сотрудники должны быть обязаны сообщать о любых подозрительных действиях или несанкционированном использовании компьютерных ресурсов. Сотрудники также должны принять необходимые меры для защиты данных и программ, находящихся под их юрисдикцией, а именно, не оставлять рабочую станцию незаблокированной в течение длительного времени. [14]

Статистика, добропорядочности сотрудников представлена на рисунке 5,

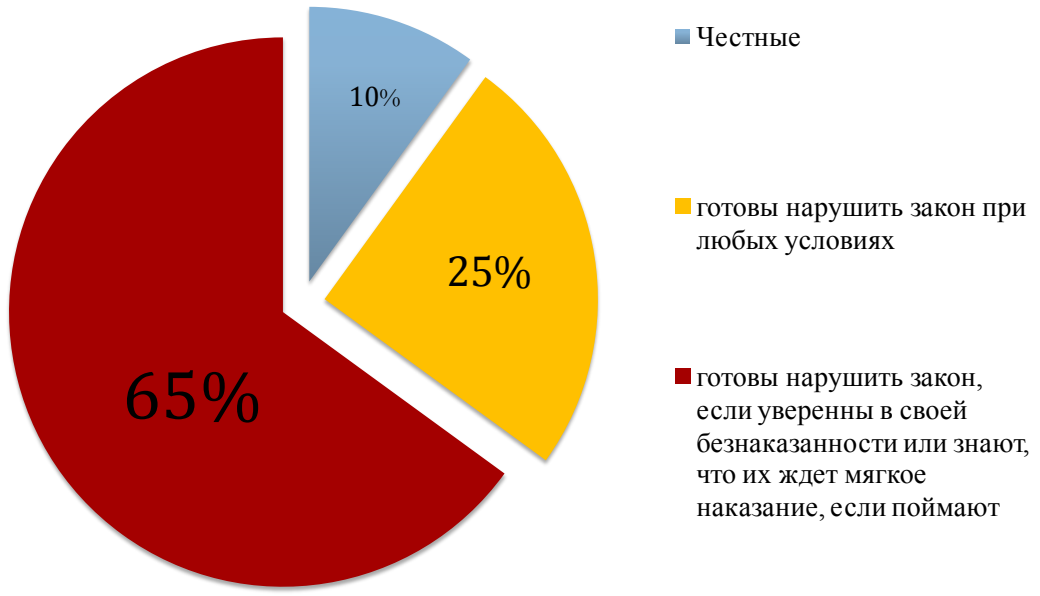


Рисунок 5 – Статистика лояльности сотрудников

Отделу кадров необходимо проводить более тщательный отбор кандидатов.

Любой сотрудник в организации всегда проходит три стадии развития:

1) устройство на работу;
2) этап работы;
3) увольнение.

При приеме на работу сотрудника необходимо собрать много информации о нем, чтобы предсказать поведение во всех ситуациях. В целом, эти проверки легче выполнить с помощью стандартных психологических

тестов. Также необходимо определить, относится ли кандидат на эту должность к одной из категорий «хлопотных работников».

3 Работа с лог данными

3.1 Понятие лога, принципы систем логирования

Лог файл или журнал событий – это файл, содержащий информацию о событиях, происходящих в системе в хронологическом порядке, сгенерированных устройством на основе заранее определенных правил. Журнал состоит из набора записей (строк), каждая запись содержит информацию о конкретном событии, происходящем в системе или сети. Основная практическая ценность лог файла заключается в том, что, используя его, мы можем воссоздать образ того, что происходит в системе, и использовать эту информацию для выявления источников ошибок, сбоев и других нежелательных событий.

Лог файлы можно классифицировать следующим образом:

1) информационный лог: нейтральное сообщение о системных фактах, позволяющее пользователю понять, что происходит в системе;
2) лог отладки: сообщения для разработчиков системы, генерирующие данные о проблемах с запуском кода приложения;
3) лог предупреждений: сообщения, относящиеся к ситуациям, которые не соответствуют системным правилам, но не влияют на общую работу программы;
4) лог ошибок: сообщения, содержащие информацию о событиях, которые вызывают различные системные ошибки. К сожалению, большинство сообщений об ошибках не дают полной картины того, что произошло, они не содержат информации о коренных причинах ошибки. [14]

Однако система не всегда правильно классифицирует события, потому что она может различать только события, критерии которых были предварительно запрограммированы. Поэтому необходимо постоянно анализировать происходящее, чтобы отслеживать и модернизировать систему.

Таким образом, сообщение журнала является своего рода информацией, записанной устройством, чтобы указать, что что-то происходит. Типичные компоненты этого сообщения:

- отметка времени;
- источник информации;
- основные данные события.

Сообщения могут иметь разные источники и протоколы записи, но компоненты, описанные выше, все равно будут присутствовать. Однако сегодня нет конкретного формата, регулирующего содержание каждой части в отдельности.

Одной из самых больших проблем в анализе логов является то, что многие сообщения, сформированы не лучшим образом и не предоставляют полезной для анализа информации либо из-за того, что информации в сообщении практически нет, либо из-за того, что сообщение наоборот переполнено различными полями и данными, в связи с чем его чрезвычайно сложно обрабатывать и получать информацию.

21 апреля 14:38:25 192.168.5.1 rlogin: соединение отказано

Анализируя это сообщение, мы не получаем никакой информации о том, почему соединение было разорвано, на каком этапе оно произошло. Мы имеем лишь факт возникновения проблемы, что, в свою очередь, полезно, но не понятно, как с этим бороться, поэтому разработчик, программируя формат лог сообщения, должен очень внимательно подходить к этому аспекту.

Стандартный протокол системного журнала наиболее распространенным методом сбора логов. Принцип системного журнала довольно прост: различные компоненты системы создают тривиальные текстовые сообщения о произошедших событиях и отправляют их на сервер системного журнала через TCP. Правила отправки и генерации сообщений о событиях называются протоколом системного журнала. Существует максимальный размер сообщения, сегодня его размер составляет 1024 байта.

На сегодняшний день Syslog – не единственный механизм генерации и отправки сообщений журнала. Например, операционная система Microsoft Windows имеет собственную систему регистрации и записывает информацию о входе в систему, выходе пользователя из системы, сообщениях приложений и других событиях в своем собственном формате хранения.

Базы данных также являются удобным способом хранения данных о событиях в системе. В этом случае сообщение, вместо того, чтобы быть сгенерированным в Syslog, немедленно записывается в реляционную базу данных. Этот механизм имеет большие преимущества, особенно с точки зрения возможности структурированного хранения и анализа информации, но очевидным недостатком этого метода является повышенное потребление ресурсов по сравнению с Syslog.

Кроме того, определенные программы и приложения имеют свои собственные механизмы и форматы регистрации. Другими словами, провайдер предоставляет собственный программный интерфейс или позволяет вам реализовать этот аспект самостоятельно. Ниже представлен список наиболее распространенных решений по генерации и хранению лог информации:

- Syslog – основанный на UDP клиент-серверный протокол;
- SNMP – протокол созданный для работы с сетевыми устройствами;
- журнал событий Windows;
- базы данных;
- Security Device Event Exchange (SDEE) – расширяемая разметка Cisco.

3.2 Основные свойства анализа лог данных

Нужно понять, какие цели можно преследовать при проверке данных, содержащихся в файлах журналов. Конечно, конкретные цели анализа могут различаться в зависимости от области, очевидно, что цели менеджеров банков и менеджеров супермаркетов будут разными, основные из них подразделяются на два типа: анализ что произошло в прошлом и анализ, чтобы предсказать, что произойдет в будущем.

Если говорить непосредственно о задачах, которые можно решать с помощью анализа лог файлов то можно отметить следующие характерные примеры:

- управление ресурсами. Довольно часто информация о проблемах использования системы появляется в файлах журнала как различные типы предупреждений или ошибок задолго до того, как возникает серьезная проблема. В результате анализ лог файлов могут предотвратить нежелательные задачи в будущем. Если система все еще отказывает, используя журнал, вы можете понять, что произошло и почему произошла ошибка в системе;
- расследование различного рода злоупотреблений службами внутренней безопасности и правоохранительными органами. В определенных ситуациях журнал может стать неотъемлемой частью ситуаций, связанных с различными видами судопроизводства или с внутренним организационным характером. Сообщения журнала содержат много полезной информации, такой как: что произошло во время инцидента, в каком хронологическом порядке произошли события. Файлы журнала также могут быть использованы для улучшения других доказательств или там, где источники информации были повреждены или удалены злоумышленником. Ярким примером является проверка сообщений электронной почты, которые можно просто удалить из почтового ящика. Например, если человек утверждает, что не получал или не отправлял сообщение, и все действия против него являются незаконными, лог–файл может указать иное;
- безопасность информации. Информационная безопасность является одним из возможных и общих направлений управления журналом. Одним из возможных приложений является все направление SIEM (информация о безопасности и управление событиями), которое включает сбор данных из различных источников, в большинстве случаев из журналов, и получение, на основе этих данных, ценная информация различных типов, касающихся систем безопасности.

3.3 Убедительность лог данных

Доказательная сила логов основана на их точности и неизменности. Суд должен убедиться, что представленные записи отражают фактические события с правильными параметрами. Кроме того, суд должен убедиться в том, что реестры не были изменены таким образом, чтобы искажать их смысл. Кроме того, вы должны заботиться о правильной интерпретации логов.

Доказательство предоставляется следующей цепочкой элементов:

1) точность фиксирования событий и генерации записей;

2) неизменность при передаче записей из программы-генератора в программу ведения журнала;

3) точность обработки записей программой ведения журнала;

4) постоянство при хранении логов до момента изъятия;

5) точность процедуры изымания;

6) неизменность при хранении, до осмотра или передачи для рассмотрения;

7) точность интерпретации.

При передаче записей из программы-генератора в программу ведения журнала ошибки, приводящие к искажению информации, не могут рассматриваться. Их вероятность ничтожна. Но вероятность недоставки одной или нескольких записей из программы-генератора в программу ведения журнала невелика. Особенно, когда эта доставка осуществляется по сети, использующей протокол syslog, который не имеет механизма для подтверждения получения сообщения. То есть на данный момент нет сомнений в правильности регистрации события, но необходимо предусмотреть возможность пропуска одной или нескольких записей.

Точность программы ведения журнала. Вероятность ошибки, связанная с искажением записи в процессе входа в систему, очень мала, но не равна нулю. Время события может или не может содержаться в самой сгенерированной записи. Эта запись передается в программу ведения журнала, которая обычно добавляет свою собственную временную метку. Ошибка в настройке часов компьютера может быть низкой, эта ошибка обычно не превышает 1-3 минут. В связи с вышеизложенным, во время экспертизы и экспертного исследования, необходимо записать показания часов с обоих компьютеров, где работает программа журнала генератор и где работает программа журнала.

Неизменность при хранении журналов. Журналы обычно хранятся в текстовом файле или базе данных. Фактически, процесс хранения не вызывает ошибок и искажений содержимого журналов. Необходимо учитывать только два фактора: возможность преднамеренного фальсификации логов человеком и уничтожение логов в конце срока хранения. Поэтому при удалении журналов или их изучении экспертом необходимо отметить права на запись для разных пользователей, а также настройки систем хранения, ротации и очистка журналов.

Сомнения в преднамеренном искажении логов не могут возникнуть только из-за наличия технической возможности их искажения. Для

обоснованности сомнений требуется наличие признаков, указывающих на доступ к журналам.

Правильность изъятия. При проверке и удалении бортовых журналов на месте без полной передачи компьютера на экспертизу возможны следующие ошибки и трудности. Журналы могут быть довольно большими-миллионы записей и многое другое. Для их просмотра и печати необходимо применять фильтры, например, программу grep. Определение "фильтрующих" выражений-простая задача только на первый взгляд. Легко сделать ошибку даже для специалиста. Журналы могут храниться в нескольких местах, например, в нескольких папках. Поэтому при запуске необходимо включить параметры, ответственные за распределение записей в хранилищах. Также важно не пропустить журнал, который может храниться в другом месте.

В протоколе осмотра должна быть представлена точная информация о точности и полноте осмотра. То есть желательно описать все возможные места хранения журналов, привести параметры программ, отвечающих за их хранение, изучить и прикрепить к протоколу в бумажной форме наиболее важные записи, а все остальные журналы, программы, параметры в полном объеме скопировать на диск и присоединить к протоколу.

Неизменность после удаления. Изъятые логи печатаются на бумаге и прилагается к протоколу, или сохраняется на компьютерном носителе, который запечатан и хранится в файле. Лучше всего объединить оба метода. Еще одной гарантией точности осмотра логов и неизменности информации после освобождения является участие в следственных действиях специально отобранных свидетелей. Все действия с компьютерной информацией выполняются различными техническими средствами. Для использования этих технических средств, конечно, нужен специалист. Но свидетели должны также понимать смысл действий, их содержание и последствия.

Сами журналы не имеют никакой доказательной ценности. Доказательства в данном деле являются "производными" от документов:

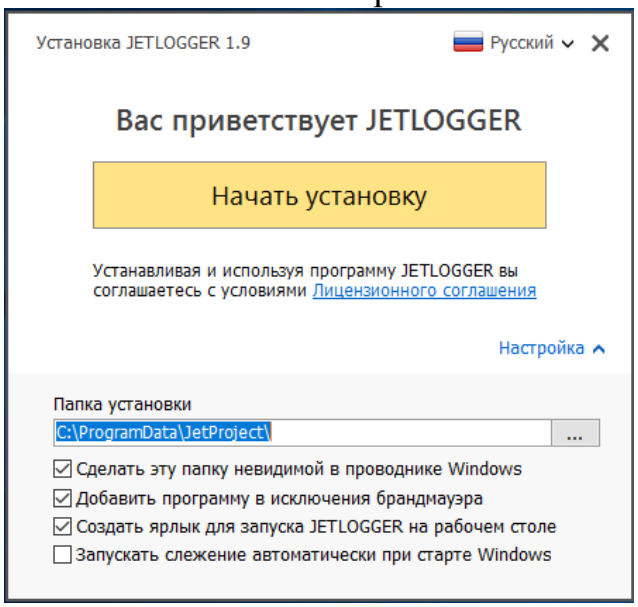
- отчет о проверке;
- экспертное заключение;
- показания свидетелей, понятых, экспертов и специалистов, касающиеся осмотра и толкования бревен.

4 Внутренний контроль сотрудников, работающих с конфиденциальной информацией.

4.1 Установка, настройка системы мониторинга активности пользователя

Программа JETLOGGER разработана для осуществления незаметного отслеживания активности пользователей на компьютере.

Установка и настройка показаны на рисунках 6 – 18.



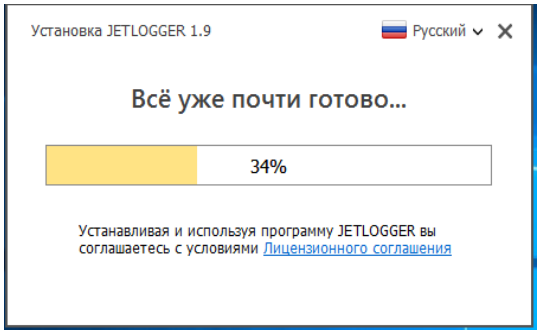


Рисунок 6 – Установка Jetlogger

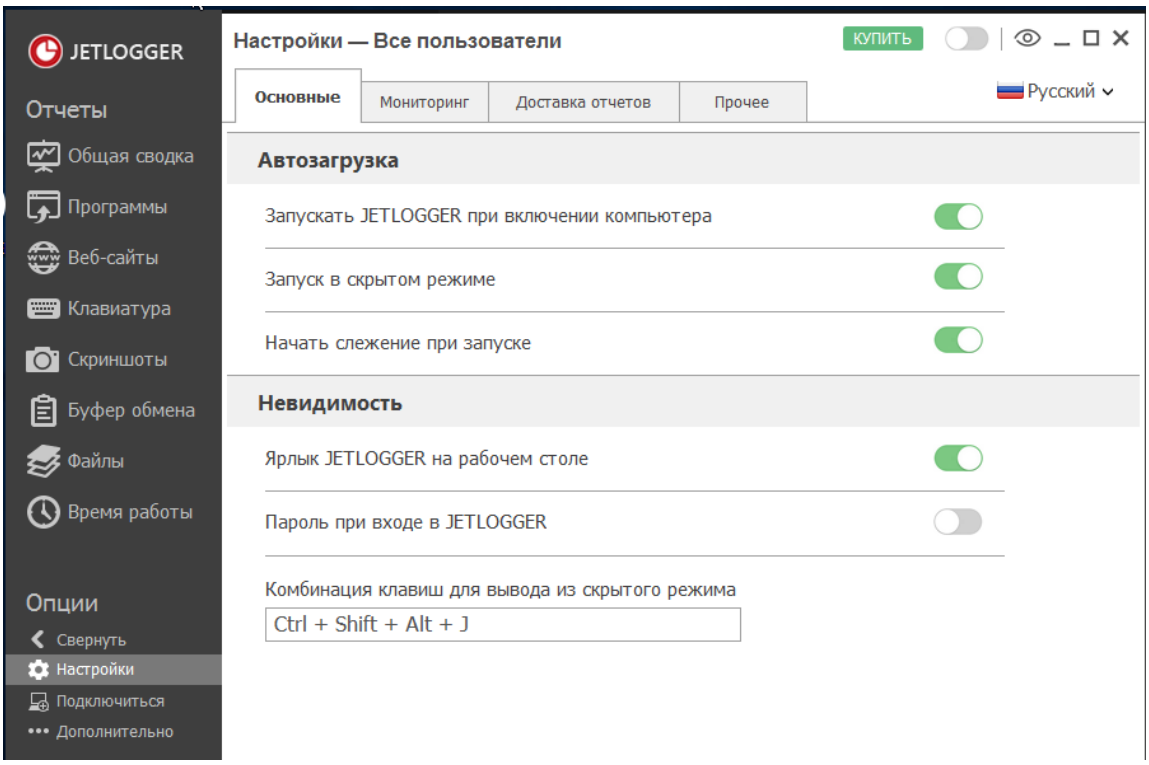


Рисунок 7 – Настройка основных параметров

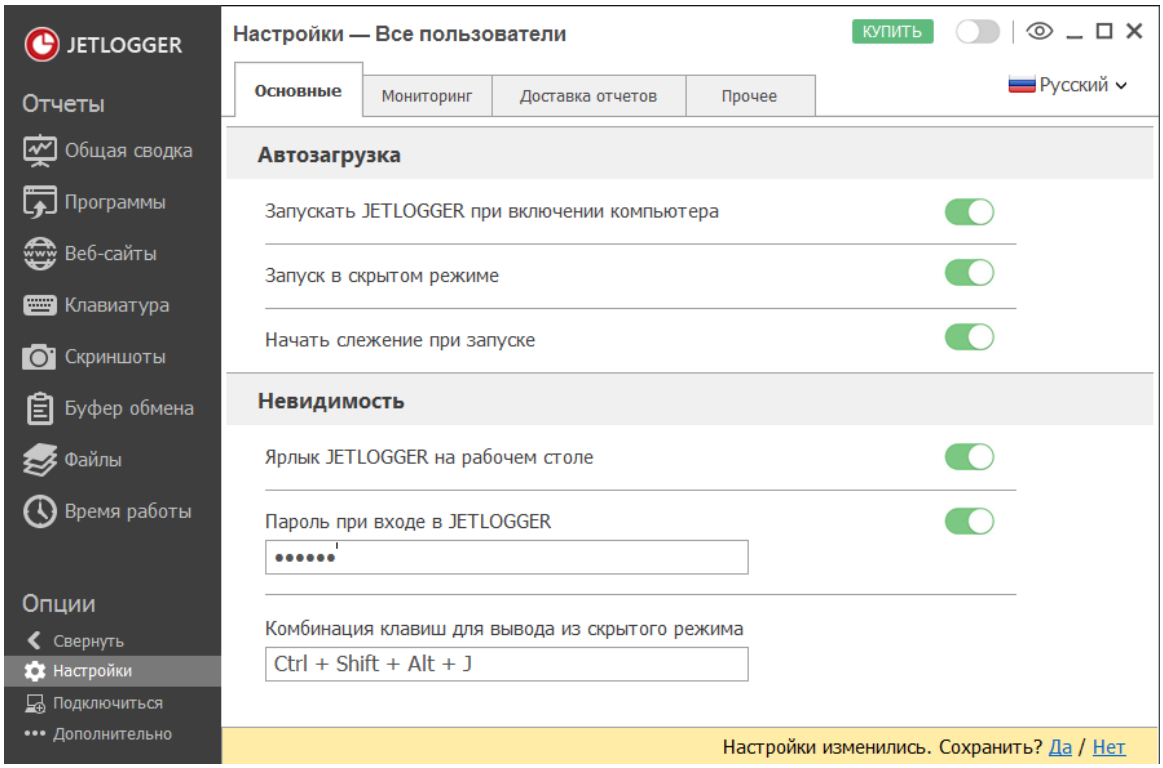


Рисунок 8 – Установка пароля для входа

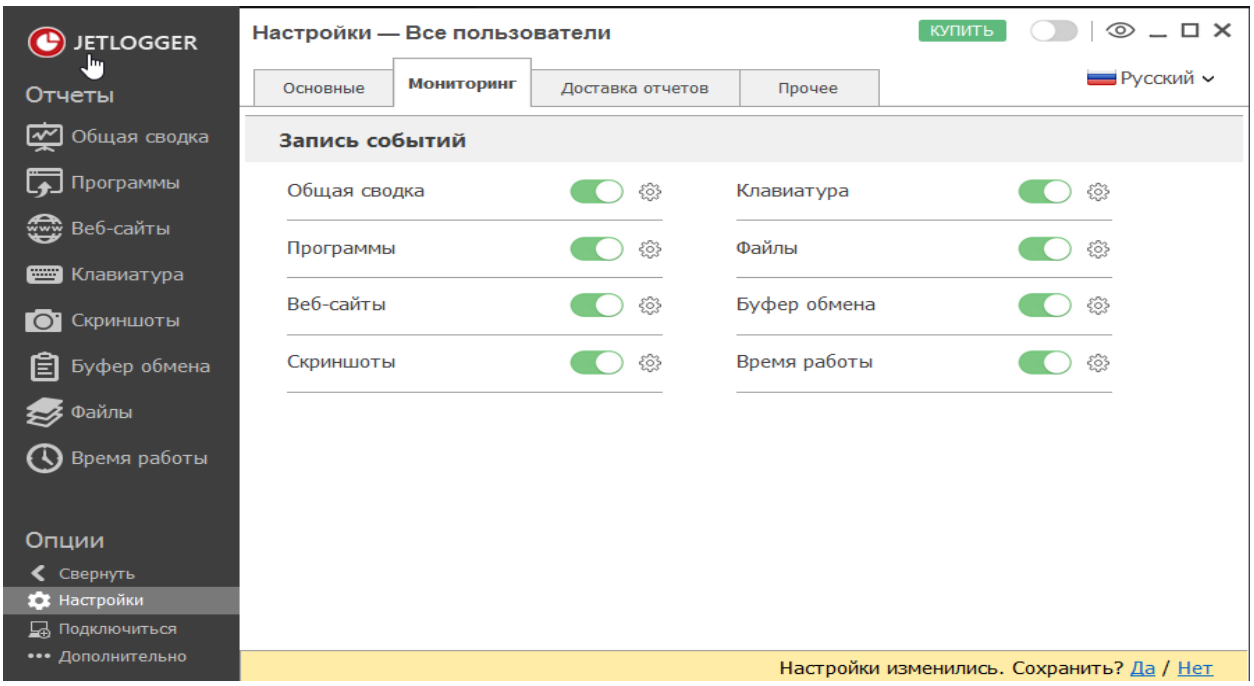


Рисунок 9 – Настройка мониторинга за системой

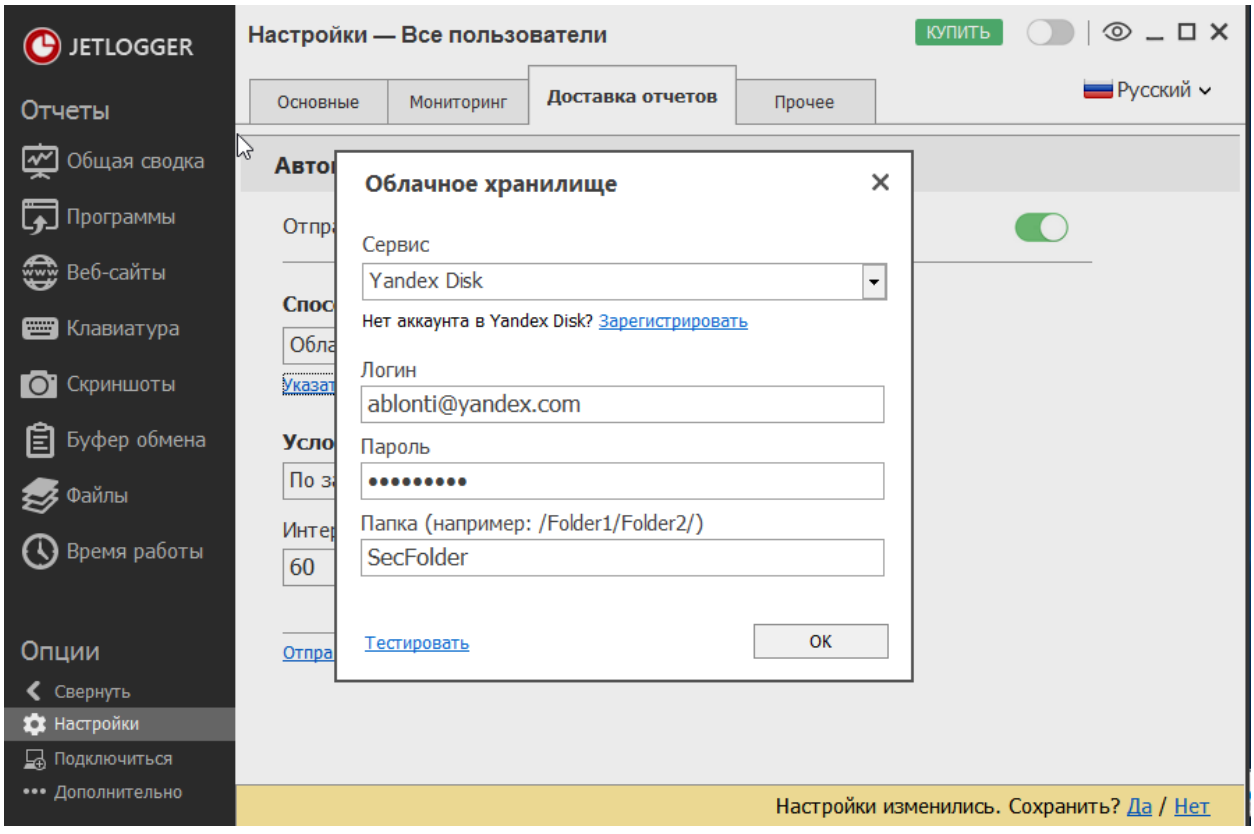


Рисунок 10 – Настройка доставки логов в облачное хранилище

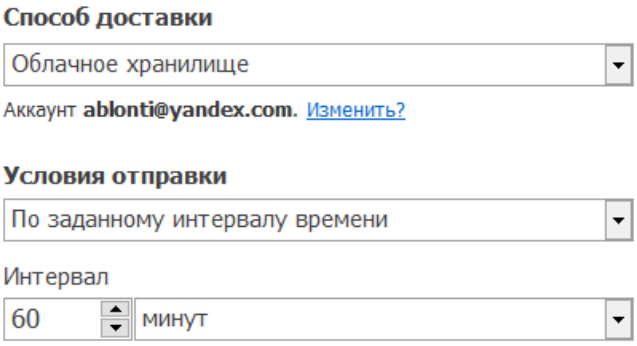


Рисунок 11 – Условия доставки логов

Так же присутствует доставка лог файлов на электронную почту, ftp сервер и в отдельную папку.

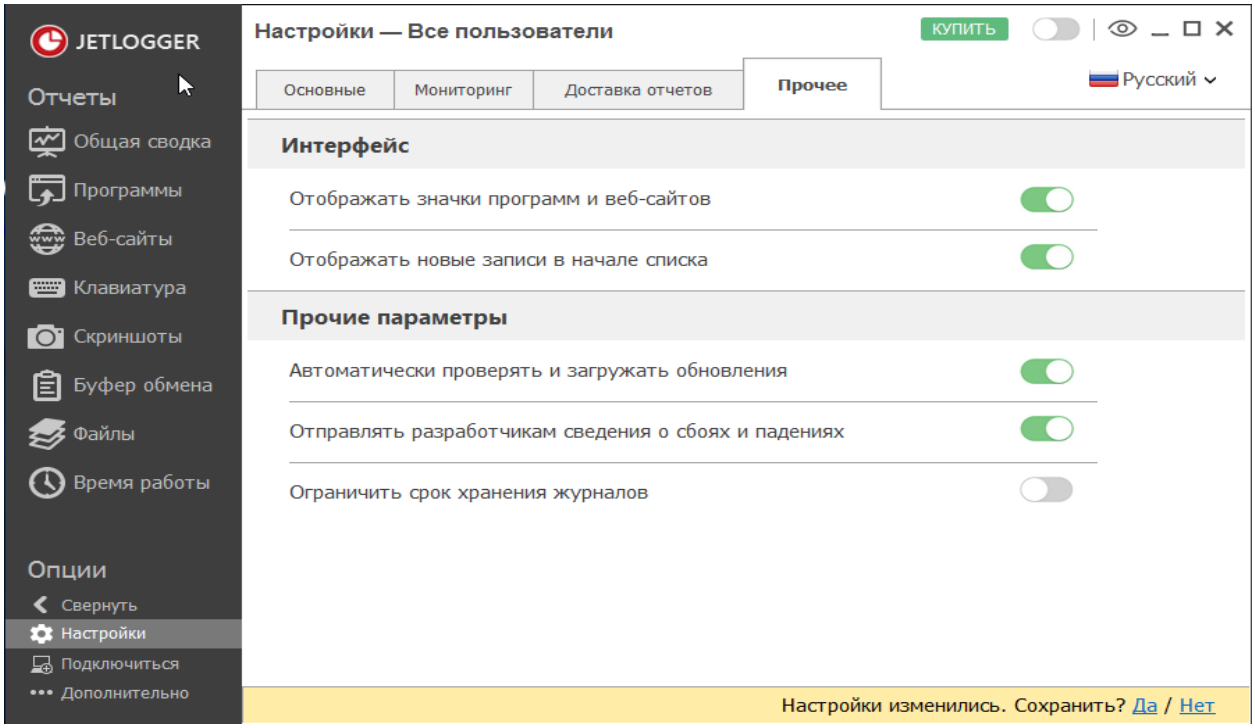


Рисунок 12 – Прочие настройки

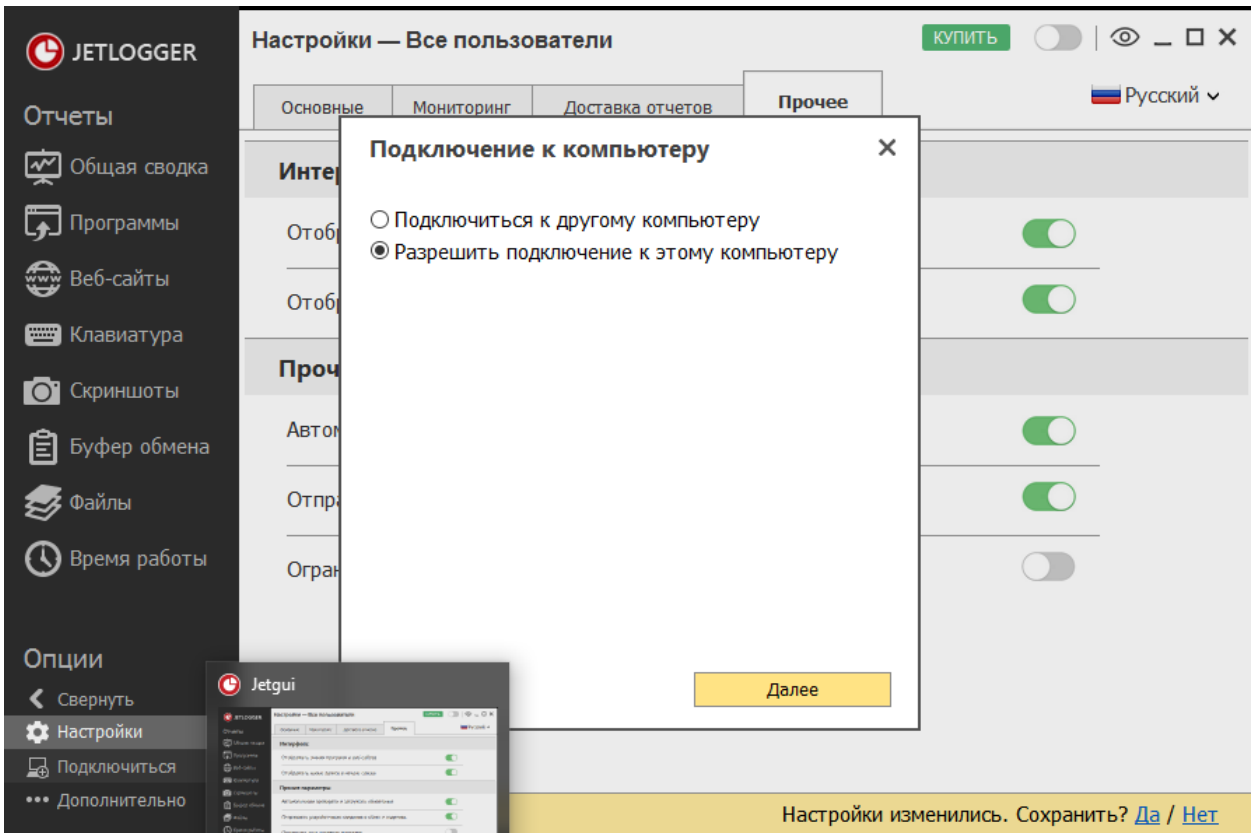


Рисунок 13 – Настройка удаленного доступа

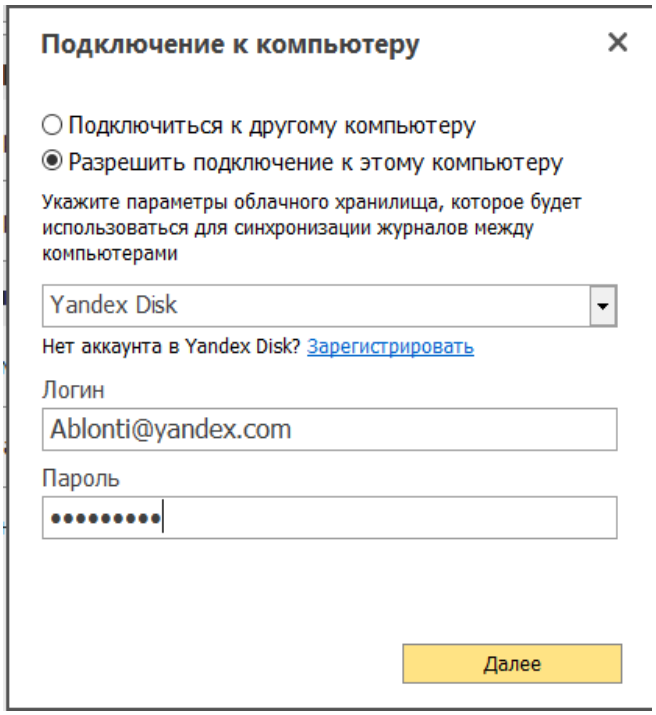


Рисунок 14 – Логин и пароль для синхронизации

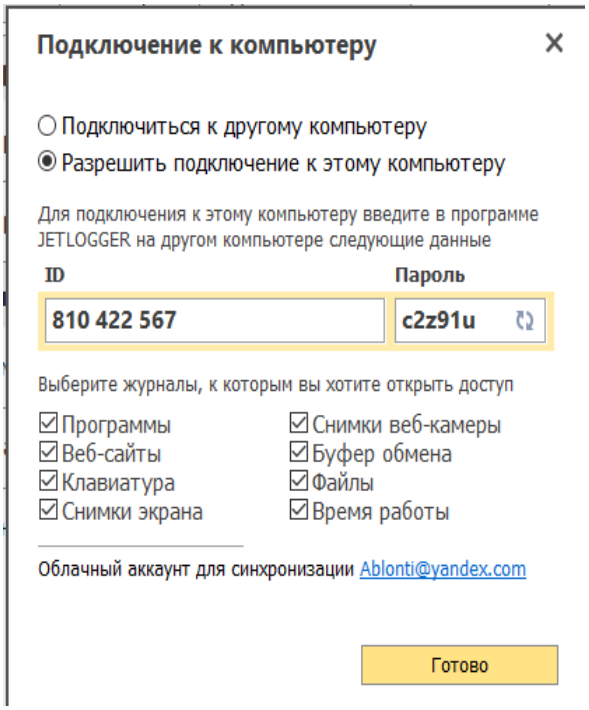


Рисунок 15 – ID и пароль для удаленного доступа

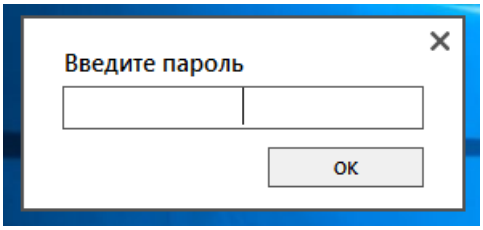


Рисунок 16 – Запуск программы с требованием ввести пароль

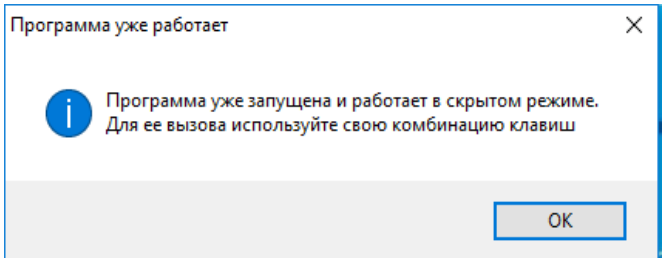


Рисунок 17 – Скрытый режим работы

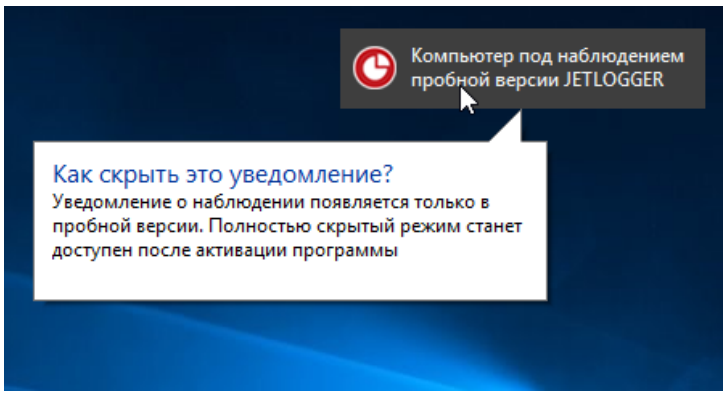


Рисунок 18 – Минус демо версии

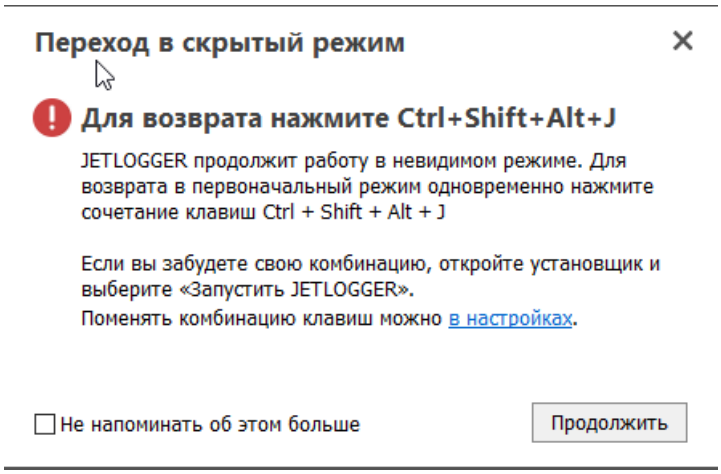


Рисунок 19 – Комбинация клавиш для выхода из скрытого режима

4.2 Мониторинг несанкционированных действий пользователей

В качестве пользовательских компьютеров были установлены в Vmware Workstation 15, 2 операционные системы это Windows 7 с именем пользователя Comp12 и Windows 10 с именем пользователя Comp1. На них были установлены и настроены системы мониторинга в точности как в предыдущей главе (Рисунок 6 – 18). В этой главе была смоделирована утечка конфиденциальной информации с рабочей станции под управлением операционной системы Windows 10 посредством почтового сервиса Gmail и действия на рабочей станции не относящиеся к рабочим. (Рисунок 20 – 37).

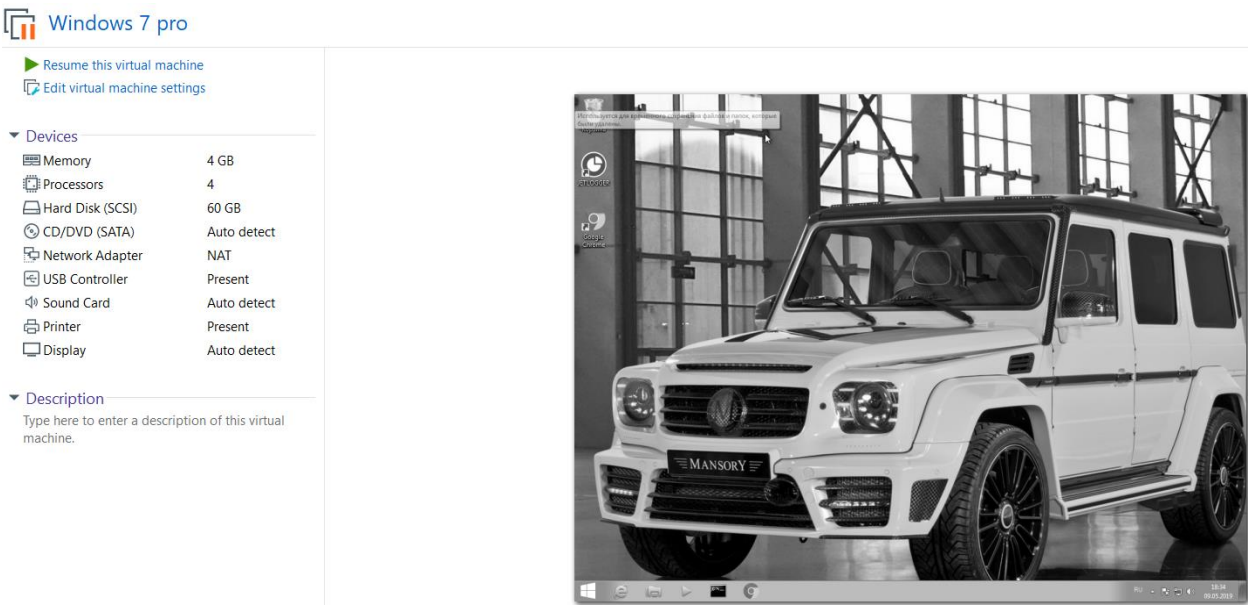


Рисунок 20 – ОС Windows 7

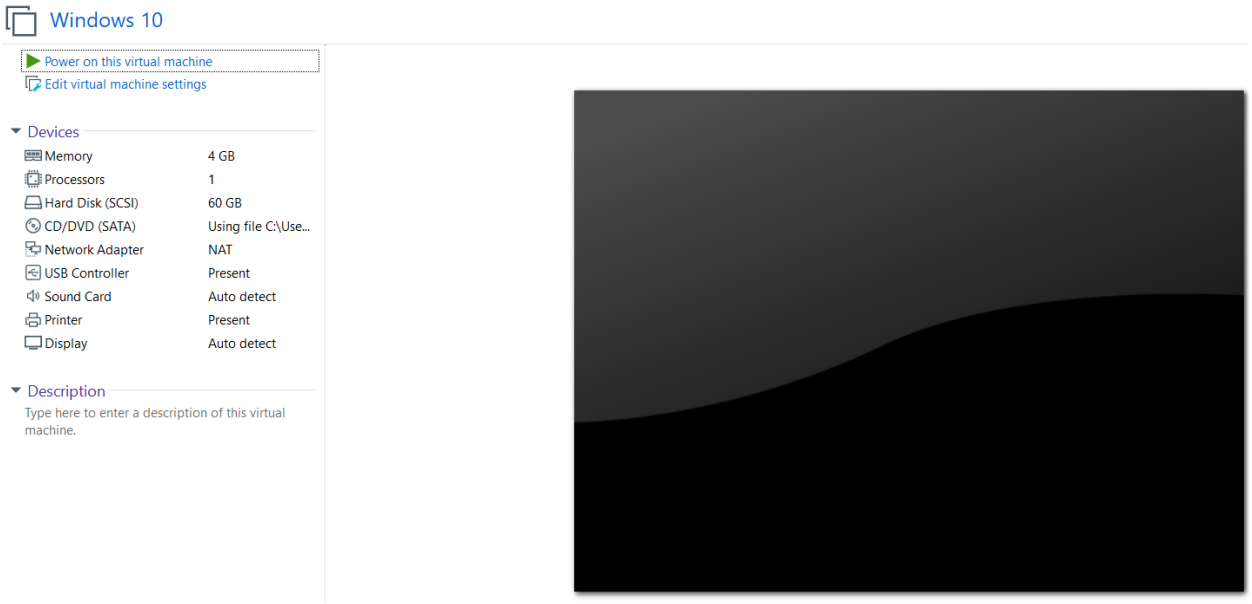


Рисунок 21 – ОС Windows 10

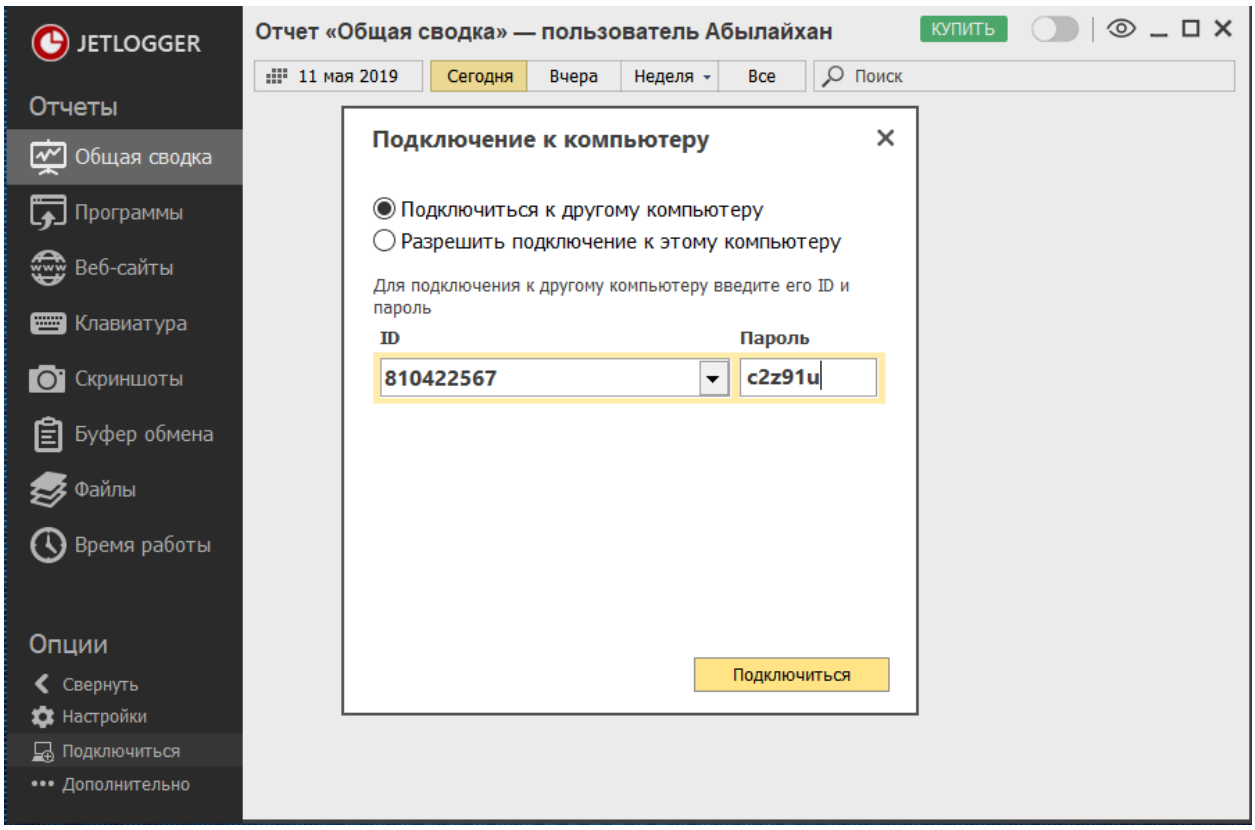


Рисунок 22 – Подключение к Windows 10 со своей рабочей станции

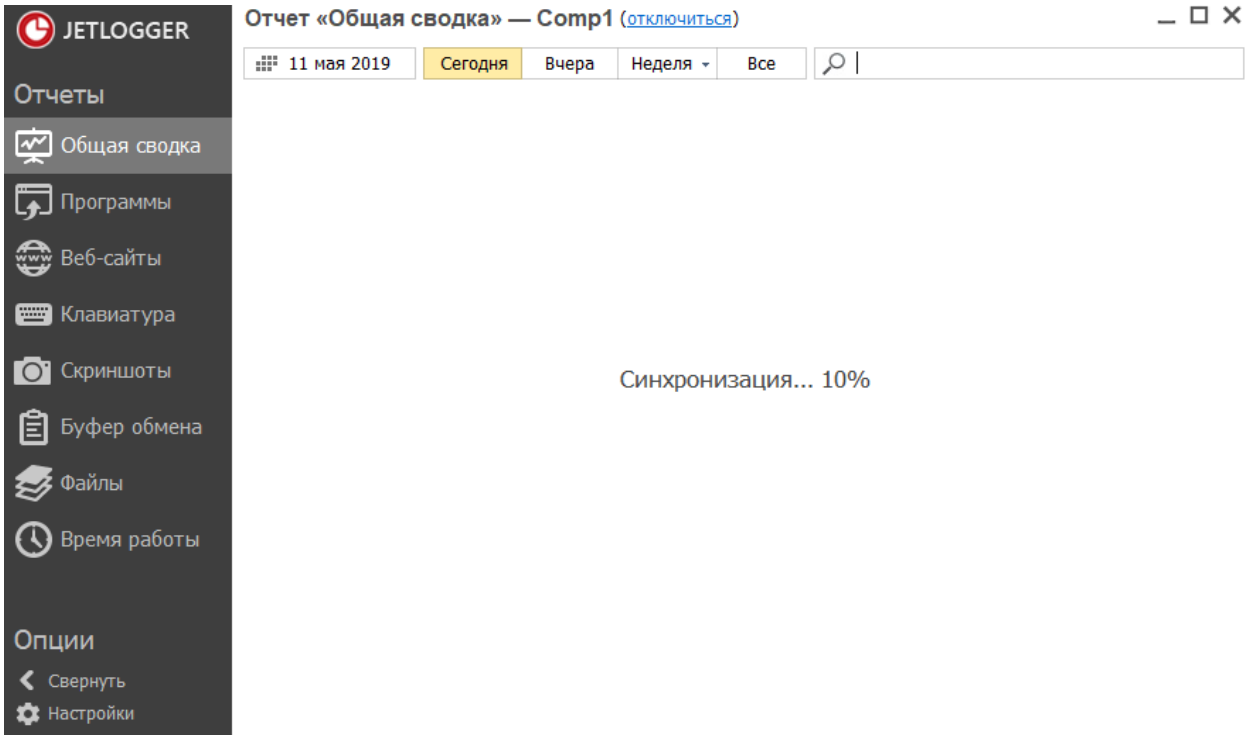


Рисунок 23 – Синхронизация

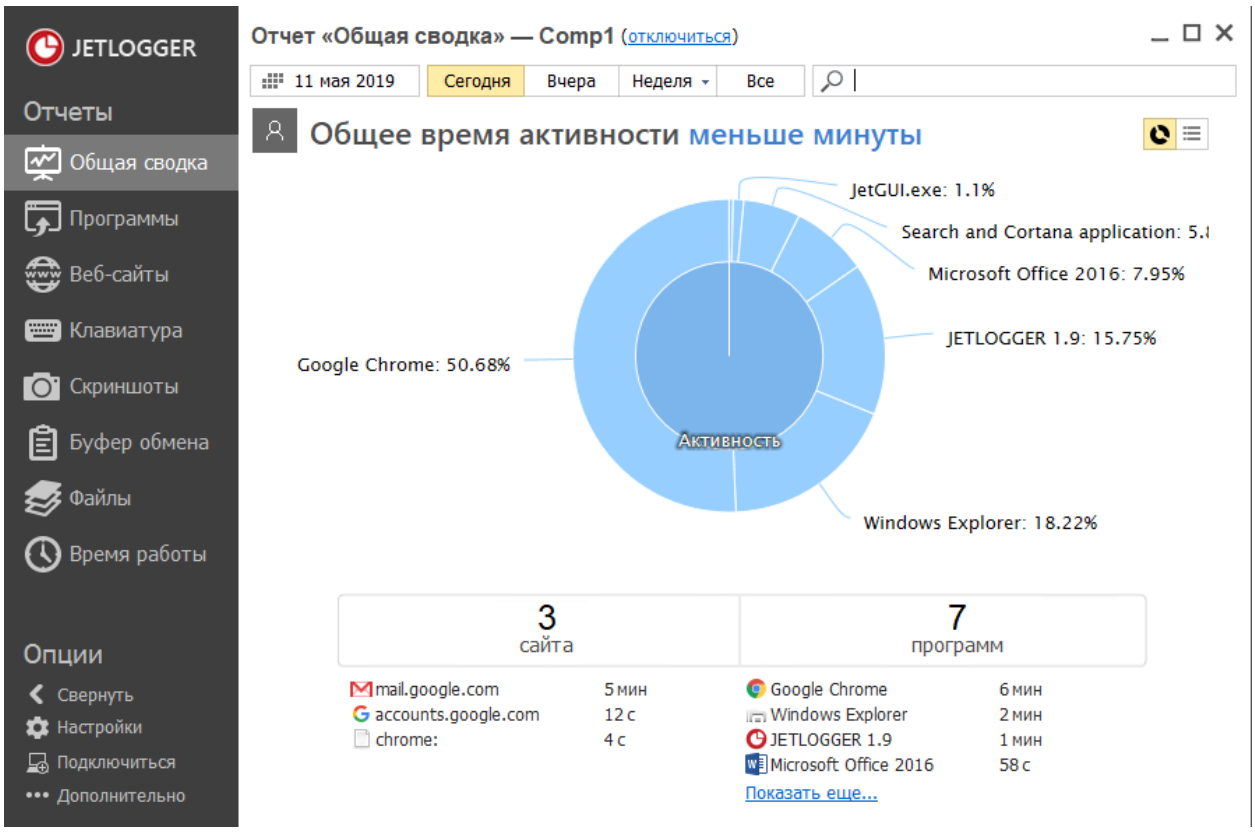


Рисунок 24 – Общая сводка активности пользователя

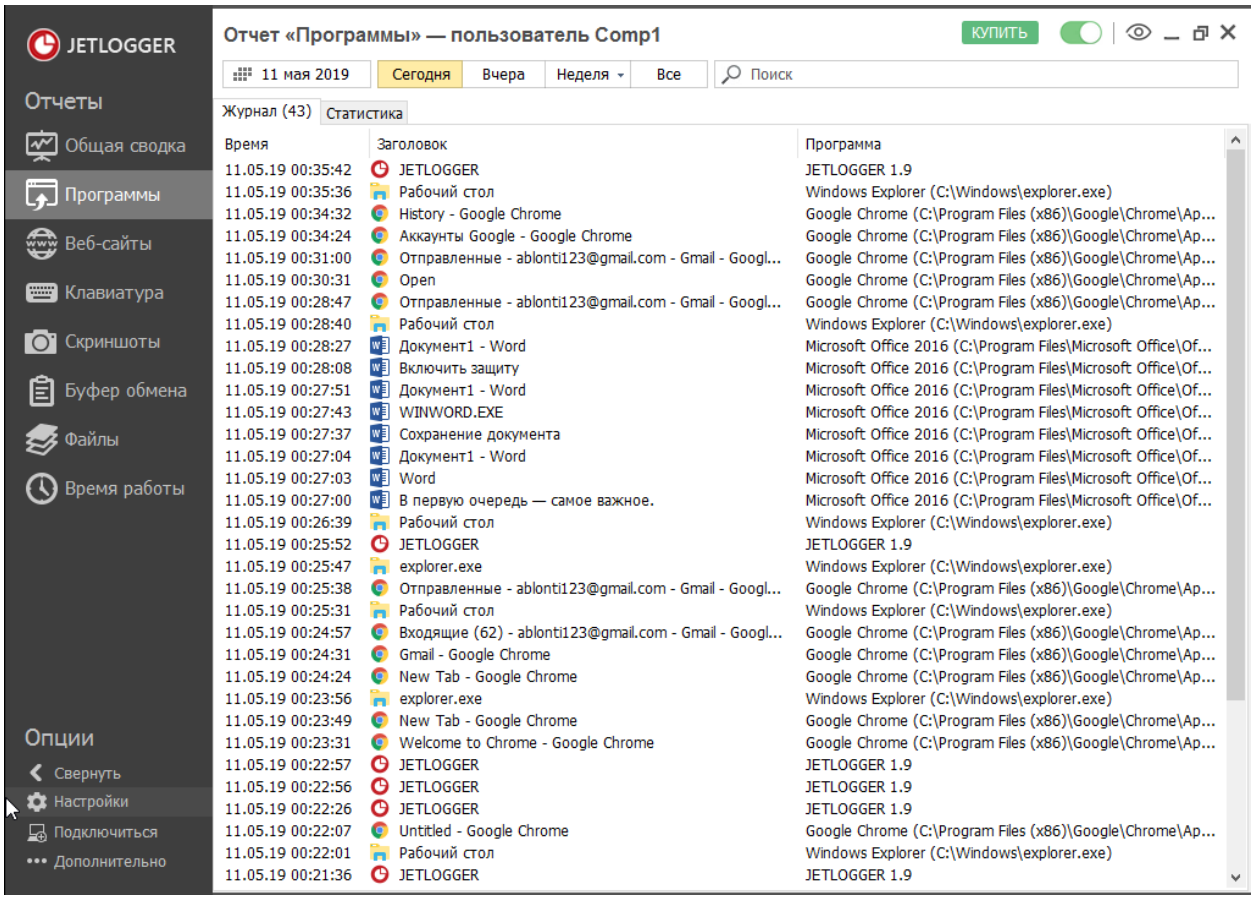


Рисунок 25 – Использованные программы

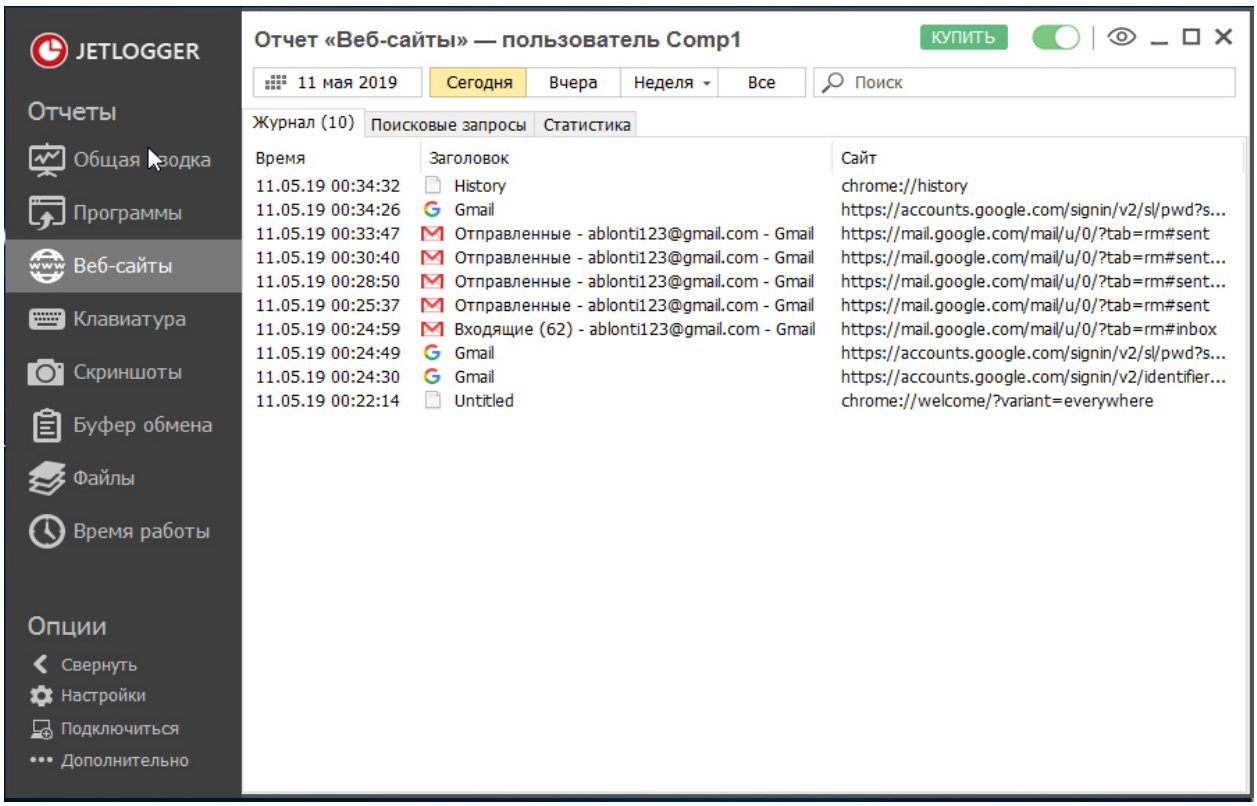


Рисунок 26 – Посещенные веб-сайты

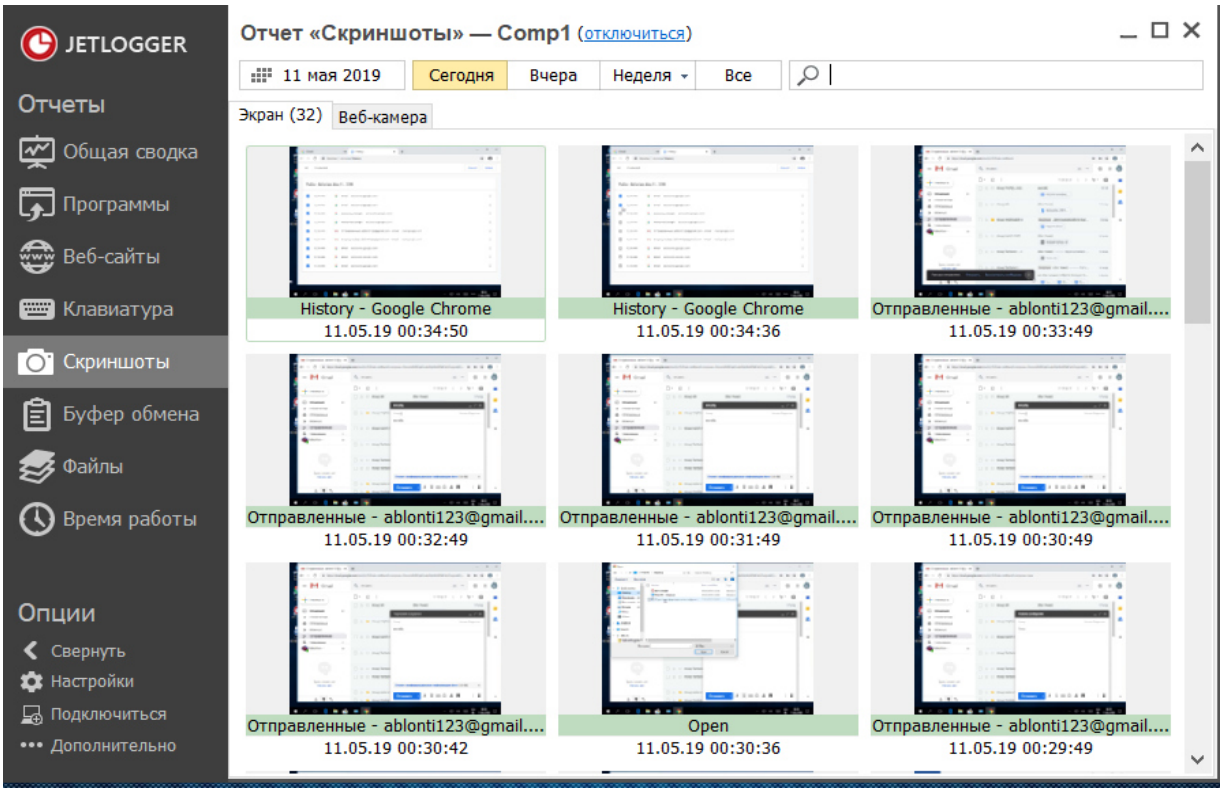


Рисунок 27 – Скриншоты с рабочей станции

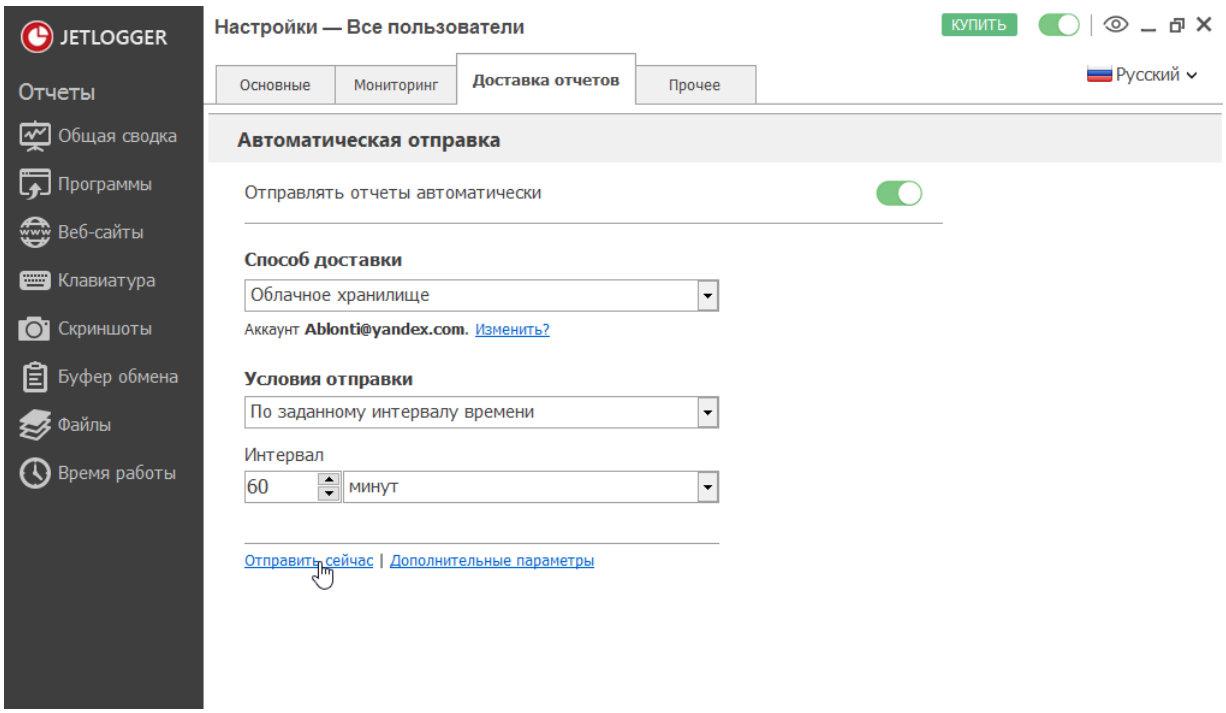


Рисунок 28 – Принудительная отправка лог файлов на облачное хранилище

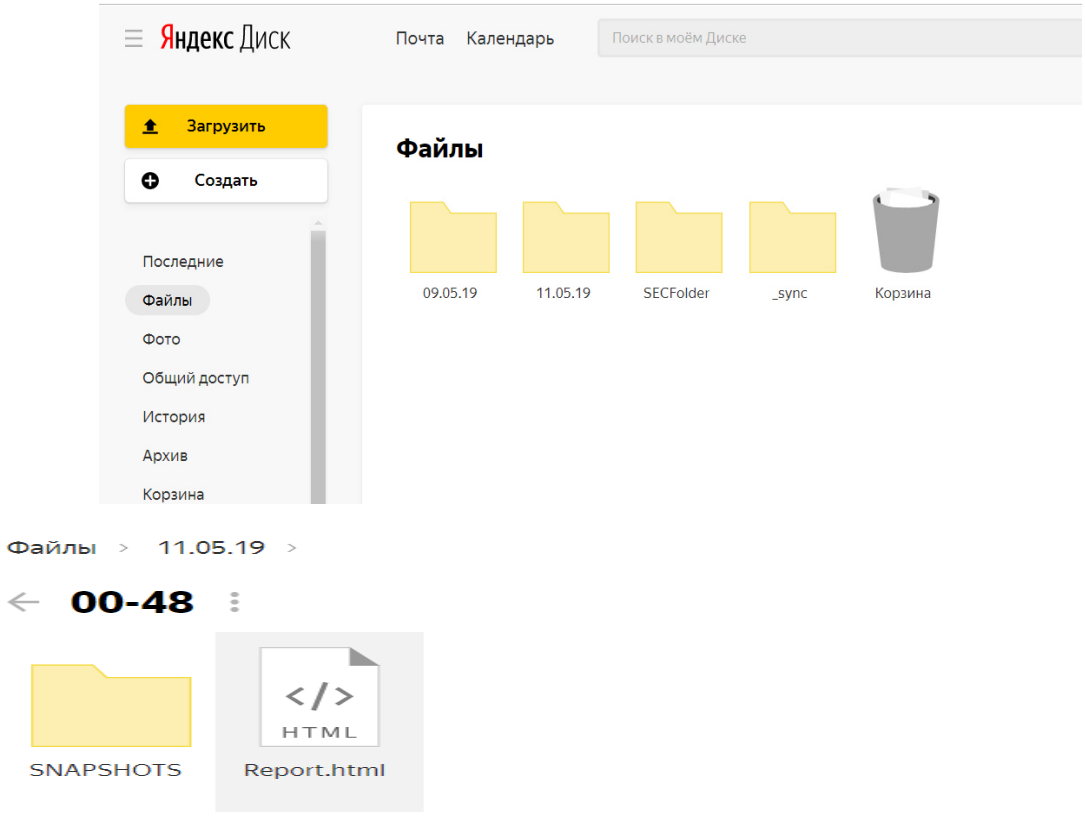


Рисунок 29 – Анализ отправленных лог файлов

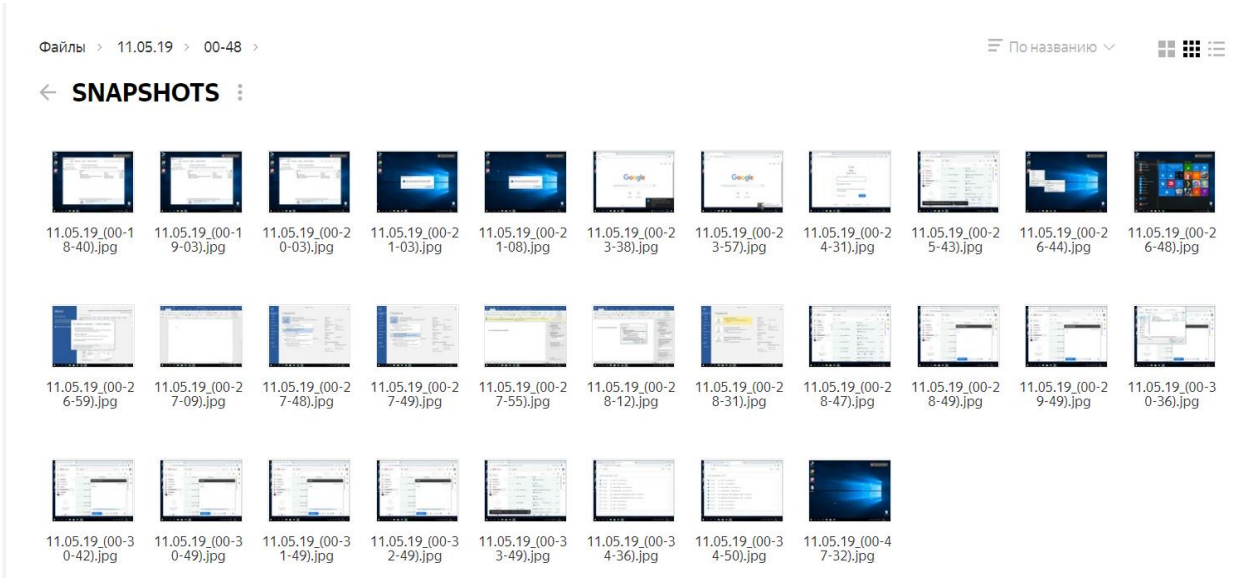


Рисунок 30 – Папка со скриншотами действий пользователя Comp1

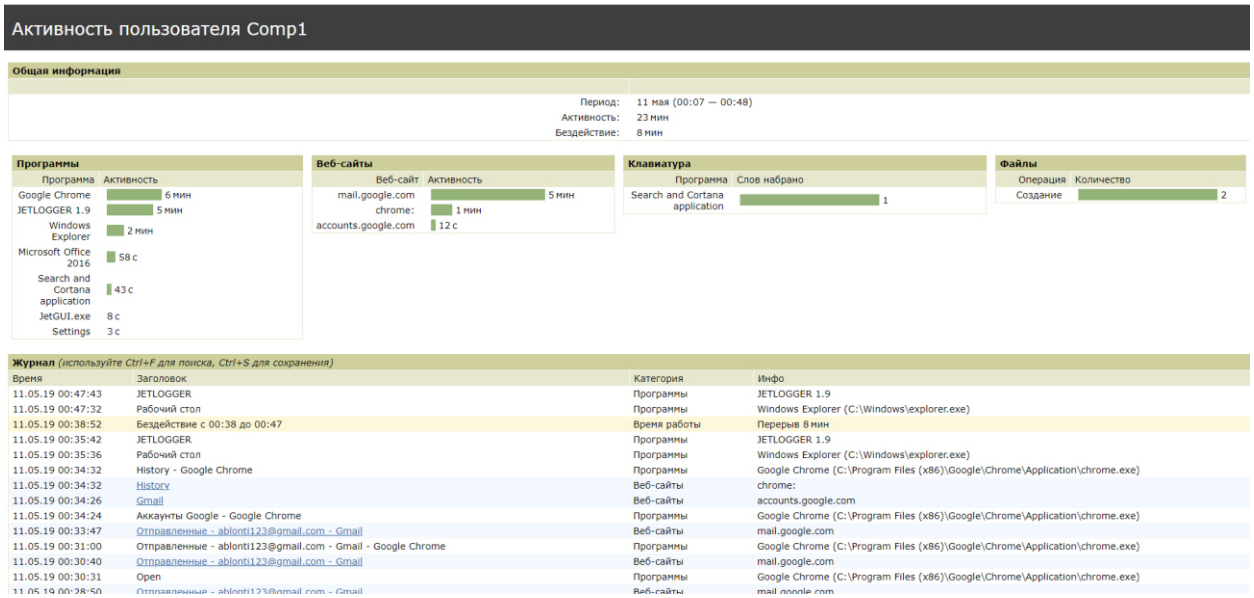


Рисунок 31 – Полный отчет активности пользователя Comp1 из файла report.html

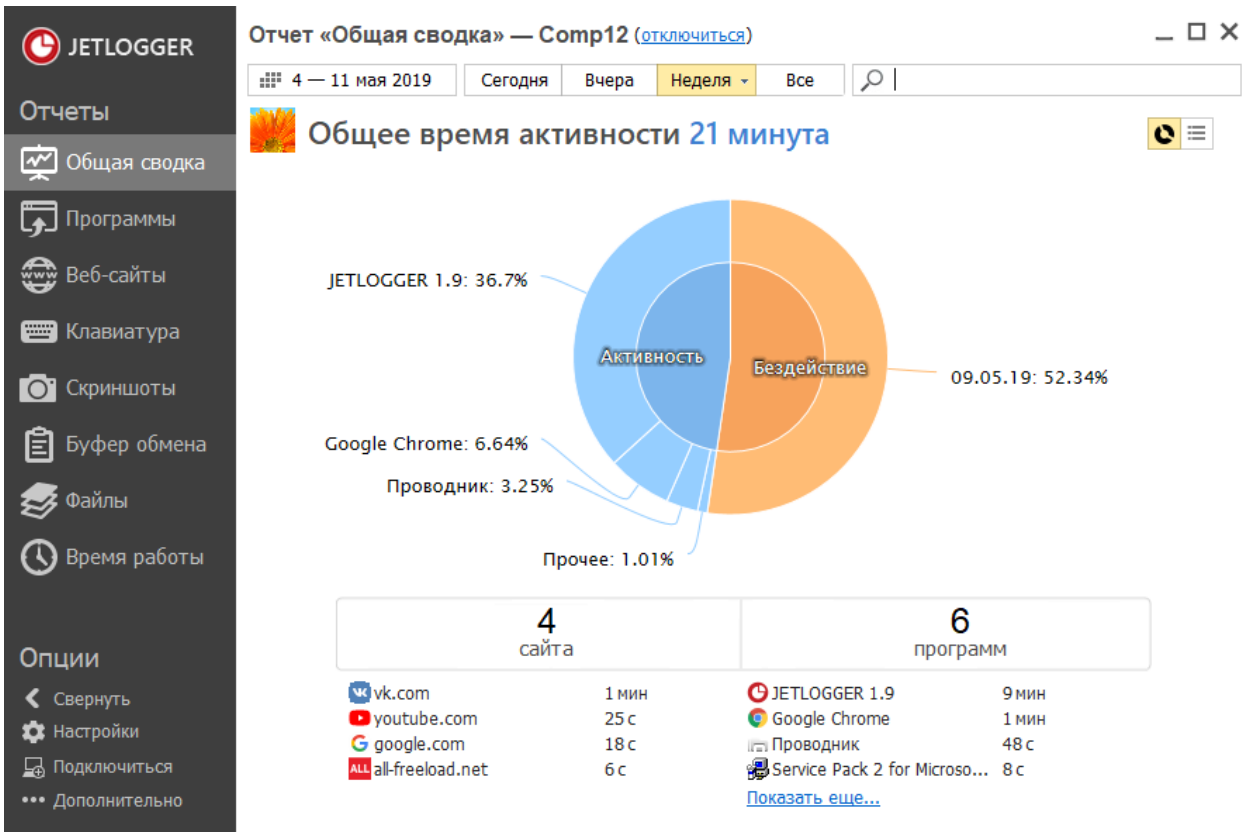


Рисунок 32 – Общая сводка активности пользователя Comp12

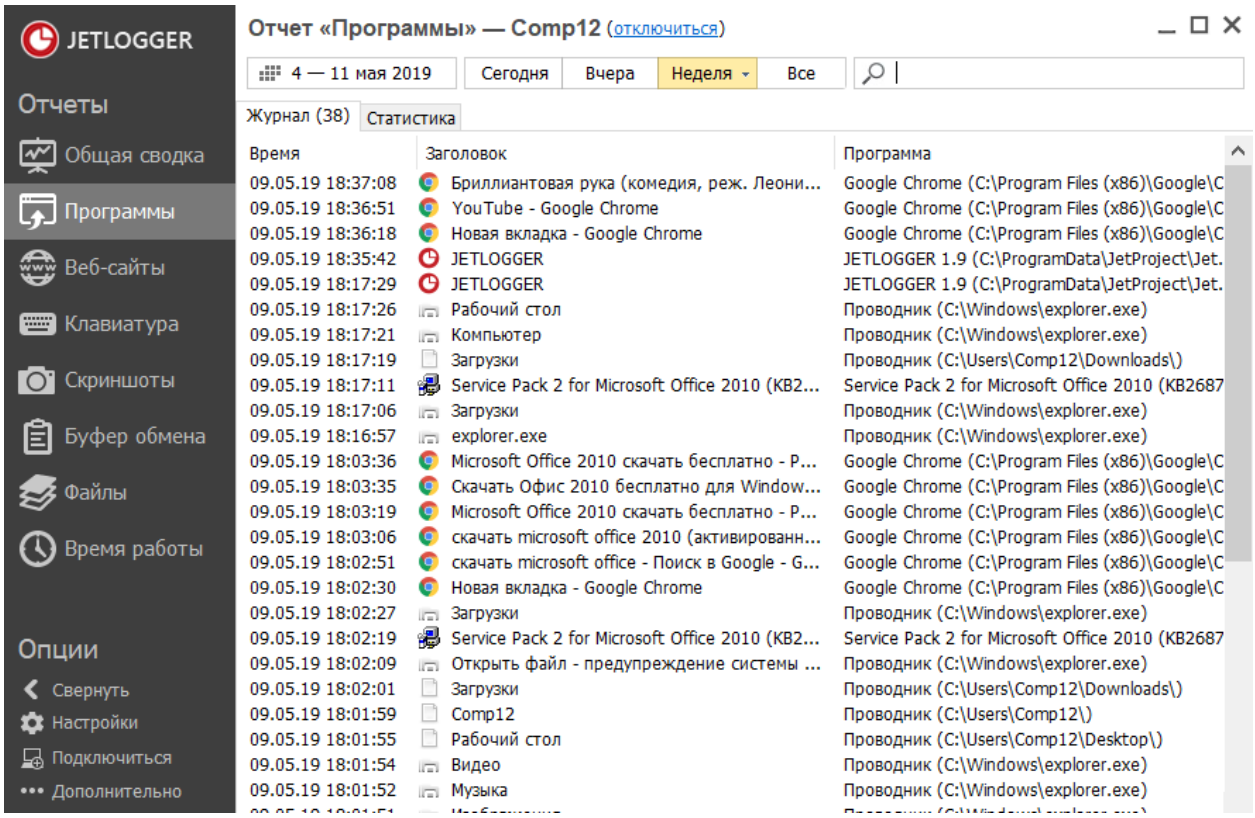


Рисунок 33 – Использованные программы пользователя Comp12

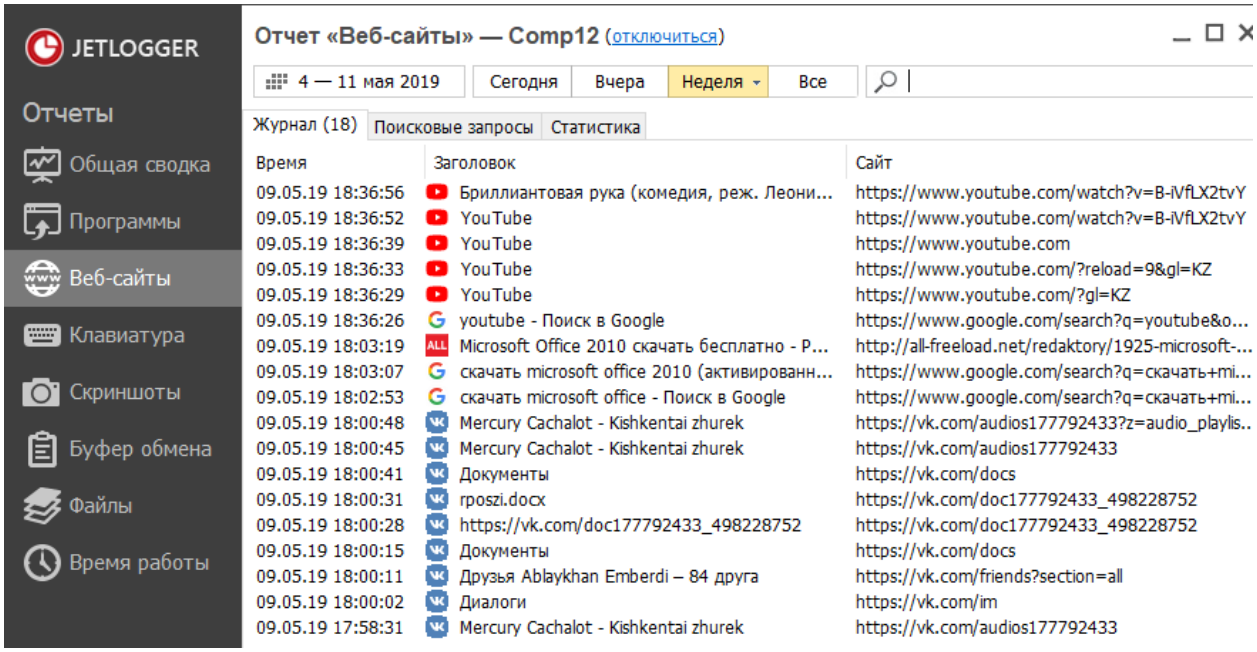


Рисунок 34 – Посещенные веб-сайты пользователя Comp12

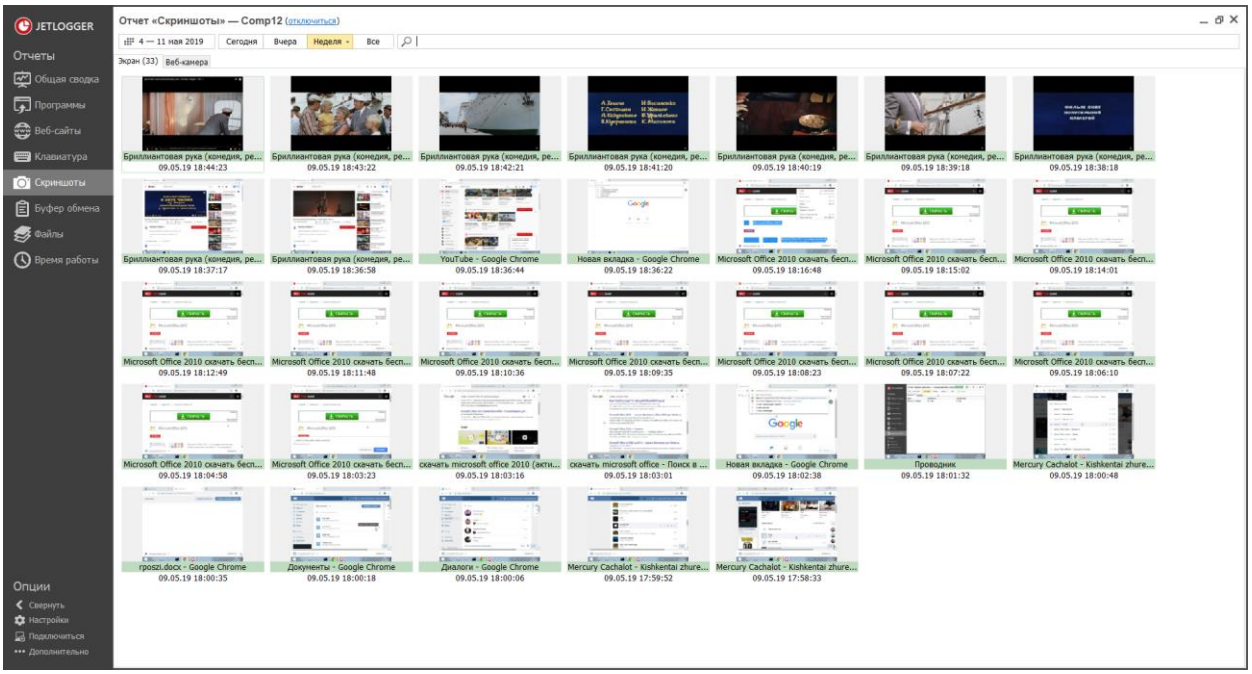


Рисунок 35 – Скриншоты с рабочей станции пользователя Comp12

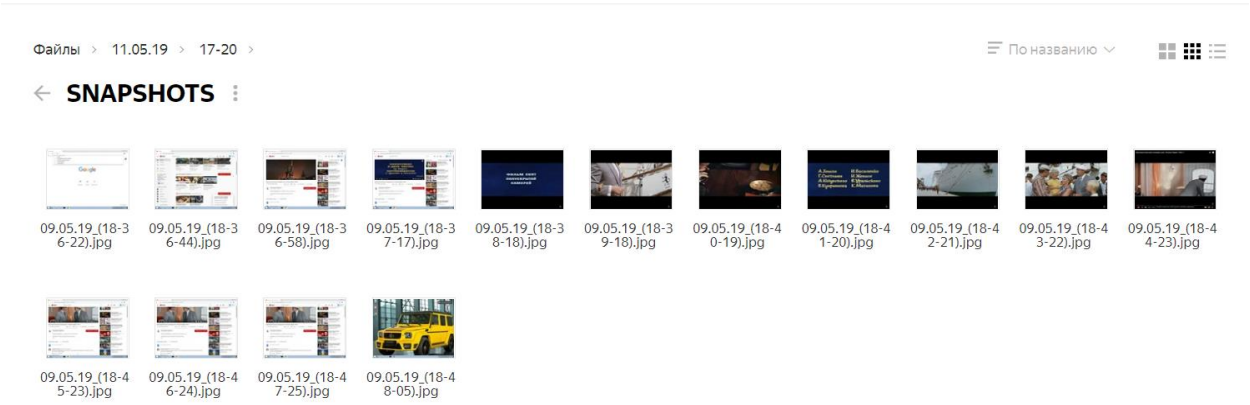
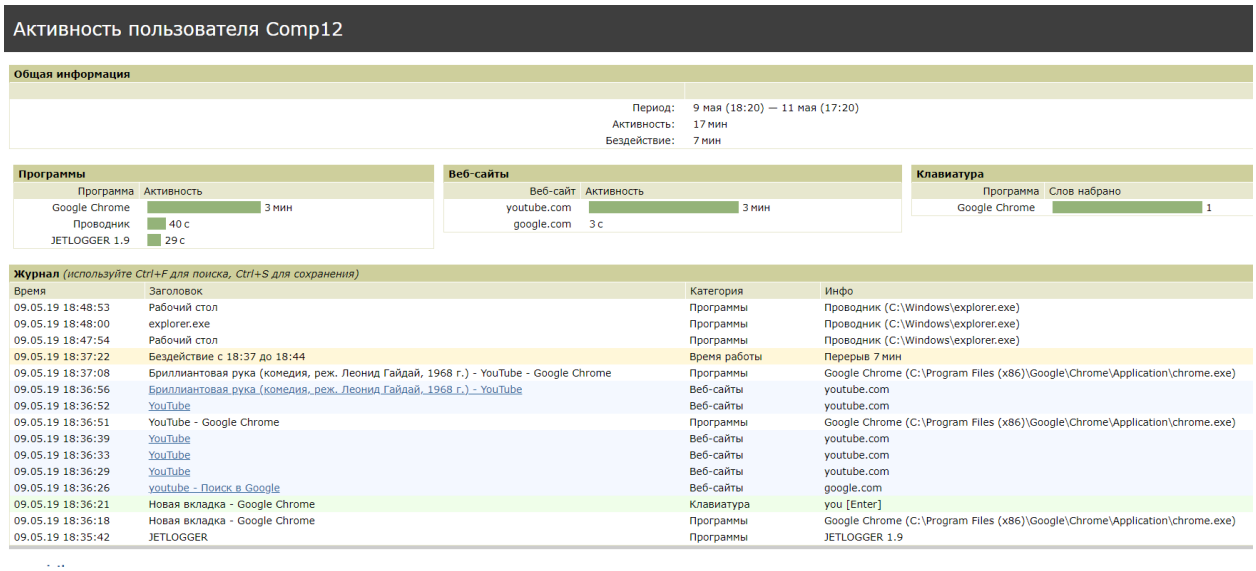


Рисунок 36 – Отправленные скриншоты пользователя Comp12



Активность пользователя Comp12

Общая информация

Период:	9 мая (18:20) — 11 мая (17:20)
Активность:	17 мин
Бездействие:	7 мин

Программы

Программа	Активность
Google Chrome	3 мин
Проводник	40 с
JETLOGGER 1.9	29 с

Веб-сайты

Веб-сайт	Активность
youtube.com	3 мин
google.com	3 с

Клавиатура

Программа	Слов набрано
Google Chrome	1

Журнал *(используйте Ctrl+F для поиска, Ctrl+S для сохранения)*

Время	Заголовок	Категория	Инфо
09.05.19 18:48:53	Рабочий стол	Программы	Проводник (C:\Windows\explorer.exe)
09.05.19 18:48:00	explorer.exe	Программы	Проводник (C:\Windows\explorer.exe)
09.05.19 18:47:54	Рабочий стол	Программы	Проводник (C:\Windows\explorer.exe)
09.05.19 18:37:22	Бездействие с 18:37 до 18:44	Время работы	Перерыв 7 мин
09.05.19 18:37:08	Бриллиантовая рука (комедия, реж. Леонид Гайдай, 1968 г.) - YouTube - Google Chrome	Программы	Google Chrome (C:\Program Files (x86)\Google\Chrome\Application\chrome.exe)
09.05.19 18:36:56	Бриллиантовая рука (комедия, реж. Леонид Гайдай, 1968 г.) - YouTube	Веб-сайты	youtube.com
09.05.19 18:36:52	YouTube	Веб-сайты	youtube.com
09.05.19 18:36:51	YouTube - Google Chrome	Программы	Google Chrome (C:\Program Files (x86)\Google\Chrome\Application\chrome.exe)
09.05.19 18:36:39	YouTube	Веб-сайты	youtube.com
09.05.19 18:36:33	YouTube	Веб-сайты	youtube.com
09.05.19 18:36:29	YouTube	Веб-сайты	youtube.com
09.05.19 18:36:26	youtube - Поиск в Google	Веб-сайты	google.com
09.05.19 18:36:21	Новая вкладка - Google Chrome	Клавиатура	you [Enter]
09.05.19 18:36:18	Новая вкладка - Google Chrome	Программы	Google Chrome (C:\Program Files (x86)\Google\Chrome\Application\chrome.exe)
09.05.19 18:35:42	JETLOGGER	Программы	JETLOGGER 1.9

Рисунок 37 – Полный отчет активности пользователя Comp12 из файла report.html

Проведя анализ отправленных скриншотов и лог–файлов с двух рабочих станций можно утверждать что, пользователь Comp12 бездельничает на рабочем месте, а пользователь Comp1 отправил конфиденциальный файл через почтовый сервис Gmail затем очистил историю браузера чем нарушил Часть 2 статьи 211 УК РК которая предусматривает ответственность за разглашение или использование сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена по работе, что в теории могло причинить крупный ущерб. Лишение свободы здесь возможно сроком от 3 до 7 лет. Обязательным условием является штраф в размере до 1000 месячных расчетных показателей.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Персонал состоит из двух работников, которые работают одновременно. В данном помещении нет шумных приборов и нынешний кондиционер поддерживает необходимую температуру, циркуляцию и влажность воздуха, поэтому можно сказать что, вентиляция и шумоизоляция рабочих мест соответствует требованиям. [15] А вот освещение здесь плохое, по этому в данной части дипломного проекта, принято решение о расчете освещения помещения.

Данное помещение, имеет длину 8 метров, ширину 5 метров и высоту 3 метра. Помещение рассчитано на 2 рабочих места.

План данного помещения показан на рисунке 5.1

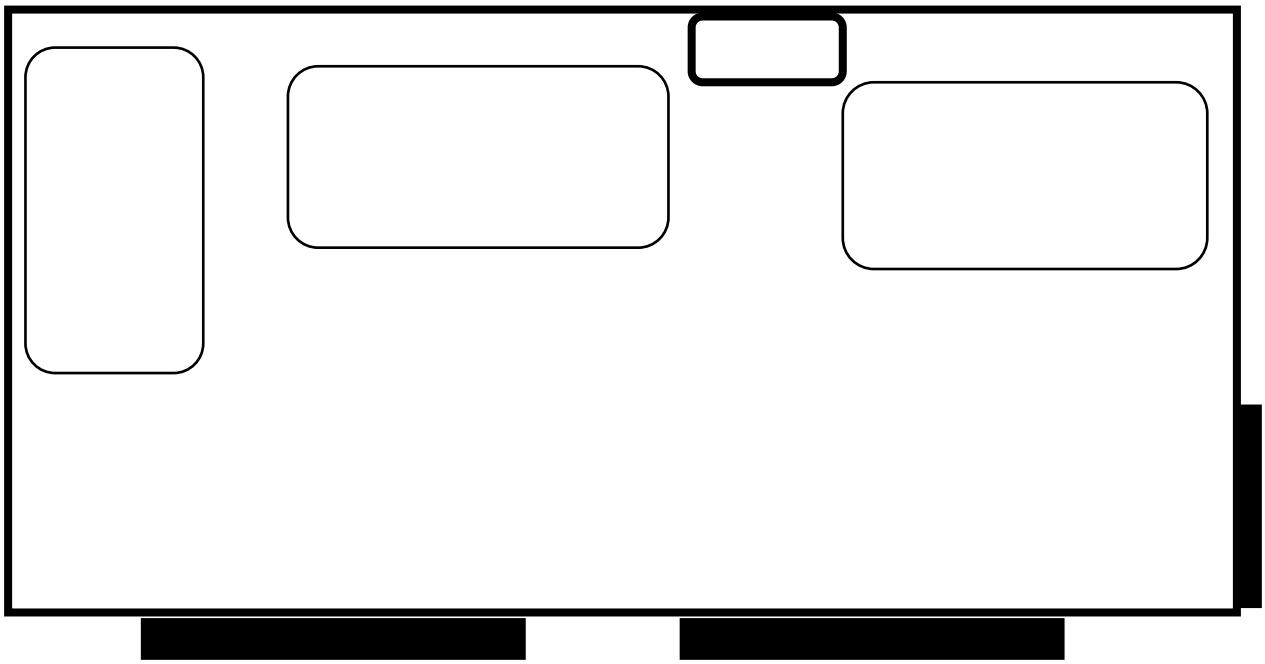


Рисунок 5.1 – План помещения

5.2 Расчет естественной освещенности

Помещение имеет такие параметры: длина L = 8 м; ширина B = 5 м; высота H = 3 м; А так же имеются два окна с размерами: ширина L_0= 1,6 м и высота H_0= 1,8 м. S_0= 2,6 м. Коэффициенты отражения потолка, стен и пола: 65%, 40%, 20%. Здание напротив находится на расстоянии $L_{зд}$= 18 м, $H_{зд}$= 16 м.

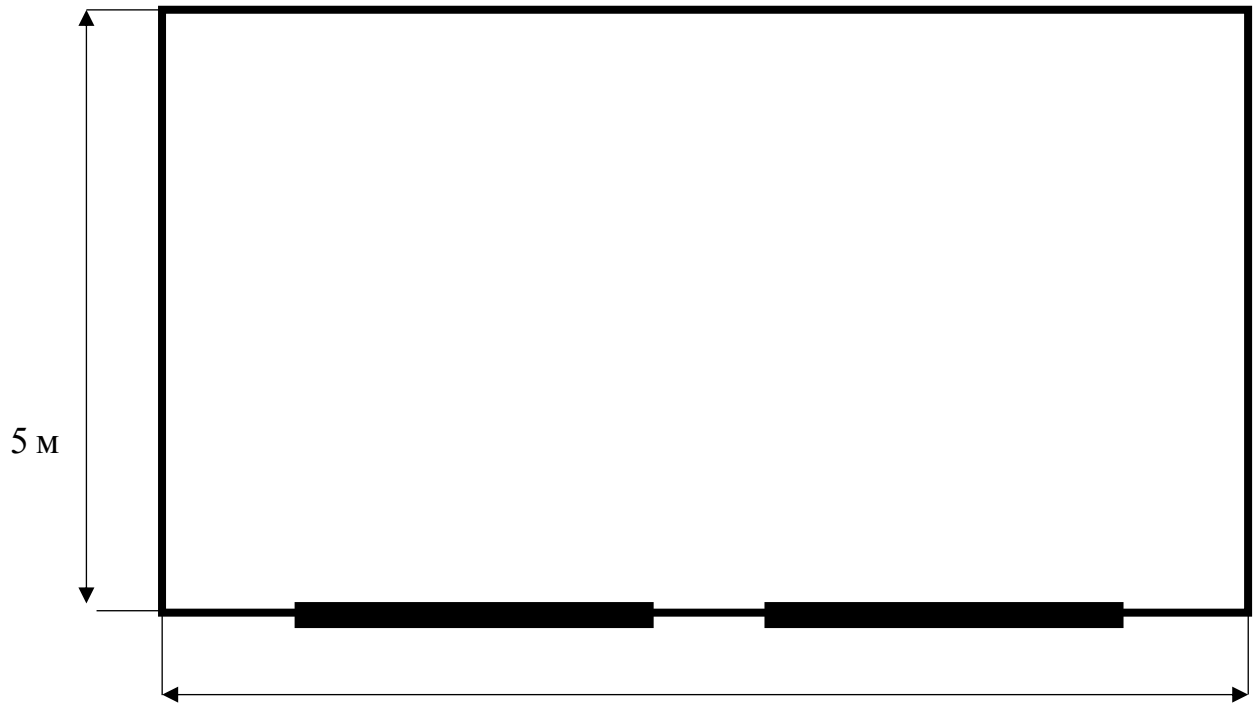


Рисунок 5.2 – Схема помещения

Проверим, достаточность площади световых проемов S_0= 2,6 м^2 для нормального освещения помещения. Расчет заключается в предварительном определении площади световых проемов при боковом освещении по следующей формуле (5.1)

$$100\frac{S_0}{S_n} = \frac{e_N \cdot \eta_0 \cdot K_{зд} \cdot K_з}{\cdot \tau_0 \cdot r_1}, \quad (5.1)$$

где S_0 – площадь световых проемов при боковом освещении, м^2;

S_n – площадь пола помещения, м^2;

e_N – нормируемое значение КЕО;

$К_з$= 1,5 – коэффициент запаса при вертикальном расположении свето–пропускаемого материала, выбираемое по СНиП II–4–79.

τ_0 – общий коэффициент светопропускания;

r_1 – коэффициент, учитывающий повышение КЕО при боковом освещении;

$К_{зд}$= 1,4 – коэффициент, учитывающий затемнение окон противостоящими зданиями, [16] принимают по таблице 5.1:

Таблица 5.1 – Коэффициент, учитывающий затемнение окон противостоящими зданиями

$L_{зд}/H_{зд}$	0,5	1	1,5	2	3 и более
$K_{зд}$	1,7	1,4	1,2	1,1	1

Площадь пола определяется по формуле (5.2)

$$S_n = B \cdot L = 5 * 8 = 40 \text{ м}^2, \quad (5.2)$$

Нормированное значение коэффициента естественной освещенности вычислим по формуле (5.3)

$$e_N = e_н \cdot m, \quad (5.3)$$

Где N – номер группы территориального района по обеспеченности естественным светом;

$e_н$= 1,5 – значение КЕО выбираемое по СНиП 23–05–95 при боковом естественном освещении;

m =0,75 коэффициент светового климата, определяется по СНиП 23–05–95

Таким образом:

$$e_N = 1{,}5 * 0{,}75 = 1{,}125\%,$$

Глубина помещения при одностороннем освещении

$$l = B - 1 = 5 - 1 = 4\text{м},$$

Для получения значения световой характеристики η_0, были рассчитаны следующие соотношения :

$$\frac{L}{l} = \frac{8}{4} = 2,$$

$$\frac{l}{h_1} = \frac{4}{2} = 2,$$

$$\eta_0 = 9.5,$$

Значение световой характеристики η_0 принимается по таблице 5.2

Таблица 5.2 – Значение световой характеристики

Отношение длины (L) к глубине (l)	Значение световой характеристики при отношении глубины помещения к его высоте от уровня условной рабочей поверхности до верха окна (h_1)							
	1	1,5	2	3	4	5	7,5	10
4 и более	6,5	7	7,5	8	9	10	11	12,5
3	7,5	6	8,5	9,6	10	11	12,5	14
2	8,5	9	9,5	10,5	11,35	15	17	17
1,5	9,5	10,5	13	15	17	19	21	22
1	11	15	16	18	21	23	26,5	29
0,5	18	23	31	31	45	54	66	–

τ0 – коэффициент светопропускания определяется по формуле (5.4)

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \qquad (5.4)$$

τ1 – коэффициент светопропускания материала: Стекло листовое узорчатое
τ1 = 0,65
τ2 – коэффициент потери света в переплетах окна:
Одинарный деревянный переплет τ2 = 0,7
τ3 – коэффициент потери света в несущих конструкциях: железобетона и дерева τ3=0,8.
τ4 – коэффициент потери света в солнцезащитных устройствах: горизонтальный козырек с защитным 15^0 углом τ4 =0,9

Тогда $\tau_0 = 0{,}65 * 0{,}75 * 0{,}8 * 0{,}9 = 0{,}351$

Определяем коэффициент r_1 – для бокового освещения по таблице 5.3

$$\frac{l}{\mathrm{h_1}} = \frac{4}{2} = 2\ ,$$

Отношение глубины помещения к ширине помещения:

$$\frac{\mathrm{L}}{\mathrm{B}} = \frac{4}{5} = 0.8$$

Отношение длины помещения к его глубине

$$\frac{L}{\mathrm{l}} = \frac{8}{4} = 2\ ,$$

Средневзвешенный коэффициент отражения потолка, стен и пола определяется по формуле (5.5)

$$\frac{P_{пот}+P_{ст}+P_{пол}}{3} = \frac{65+40+20}{3} = 42\% = 0{,}42, \quad (5.5)$$

$$r_1 = 1$$

Таблица 5.3 – Значение коэффициента r_1 для бокового освещения

Отношение глубины (l) к высоте уровня условной рабочей поверхности до верха окна (h_1)	Отношение глубины (l) к ширине помещения (B)	Средневзвешенный коэффициент отражения пола, стен и потолка, $\rho_{ср}$		
		0,4		
		Отношение длины помещения (L) к его глубине (l)		
Свыше 2,5	0,1	0,5	1	2
До 3,5	0,2	1,12	1,01	1,01
	0,4	1,28	1,25	1,20
	0,6	1,95	1,86	1,67
	0,8	1,04	1,04	1,03
	1	1,14	1,12	1,1

Подставим все найденные значения в расчетную формулу (5.1):

$$S_0 = \frac{40 \cdot 1{,}125 \cdot 1{,}5 \cdot 9{,}5 \cdot 1{,}4}{100 \cdot 0{,}351 \cdot 1} = 25{,}85 \text{ м}^2 \approx 26 \text{ м}^2$$

$$S_0 = 26 > S_ф = 5.1$$

Вывод: В данном помещении была проверена площадь светового проема которая составляет 26м^2. Из этого следует сделать вывод, что в вечернее время а так же в зимний период времени требуется дополнительные источники света.

5.3 Расчет искусственного освещения

В помещении искусственное освещение осуществляется с помощью трех светильников типа TLP235 в котором применяются люминесцентные лампы типа ЛЛ Т7 G12 по 55 Вт со световым потоком 3020 лм. Рассчитаем количество светильников, необходимых для создания освещенности в 300 лк.

Для определения количества светильников используем формулу (5.6)

$$N = \frac{E*S*Z*K_з}{F*\eta*n}, \quad (5.6)$$

Где Z – коэффициент неравномерности освещения, равный $1{,}1 \div 1{,}2 \approx 1{,}15$;

n = 2 – количество ламп в светильнике;

η – коэффициент использования светового потока;

Для определения коэффициента использования η необходимо по формуле 5.7 определить индекс помещения:

$$i = \frac{A*B}{h_1*(A+B)} = \frac{8*5}{2*(8+5)} = 1{,}54 \quad (5.7)$$

Определяем группу светильника и находим η = 0,75 по таблице 5.4

Таблица 5.4 – Коэффициент использования светового потока люминесцентных ламп

Потолок	80	80	80	70	50	50	30	0
Стены	80	50	50	50	50	30	30	0
Пол	30	30	10	20	10	10	10	0
0,6	65	43	34	41	40	34	33	28
0,8	74	53	43	50	48	42	41	36
1	81	60	49	57	54	48	48	42
1,25	87	69	57	64	61	56	55	49
1,5	91	74	62	69	65	60	59	54
2	96	82	68	76	70	66	65	60
2,5	100	87	73	80	74	71	70	65
3	102	92	77	84	78	75	73	69
4	105	96	80	87	80	78	76	72
5	106	99	83	90	82	80	79	75

При расчете по указанному методу необходимый световой поток лампы определяется по формуле (5.8)

$$F = \frac{E_{min}*S*Z*K_з}{N*n*\eta}, \quad (5.8)$$

Где E_{min} – минимальная нормированная освещенность, лк;

$К_з$ – коэффициент запаса;

S – освещаемая площадь, м^2;

Z – коэффициент неравномерности освещения;

n – число ламп;

η – коэффициент использования светового потока;

Для того чтобы проверить достаточно ли искусственное освещение, нужно рассчитать E_{min} должно быть больше 300 лк.

$$E_{min} = \frac{3020 * 3 * 2 * 0{,}75}{40 * 1{,}1 * 1{,}4} = 220{,}6$$

По расчетам E_{min} меньше чем должна быть. Поэтому нужно решить эту проблему, желательно с минимальными затратами. Было решено поменять старые люминесцентные лампы мощностью по 55 Вт со световым потоком 3020 лм на новые люминесцентные лампы мощностью по 85 Вт со световым потоком 3600 лм.

При помощи формулы (5.6) определяем необходимое количество светильников для создания освещенности в 300 лк, используя новое значение светового потока, равного 3600 лм

$$N = \frac{E * S * Z * K_з}{F * \eta * n} = \frac{40 * 1{,}4 * 1{,}1 * 300}{3600 * 2 * 0{,}75} = 3{,}42 \approx 4 \text{ светильника}$$

Значит для создания освещенности в 300 лк с разрядом зрительных работ III необходимо 8 ламп в 4 светильниках с мощностью 85 Вт и световым потоком F = 3600лм.

Определим высоту подвеса светильников над рабочими столами по формуле (5.9)

$$h_{\text{расч}} = H - \left(h_{\text{р.п}} + h_{\text{св}}\right), \qquad (5.9)$$

Где $h_{\text{св}}$= 0,35 – высота свеса ламп, м;

$h_{\text{р.п}}$= 1 – расстояние рабочей поверхности над полом, м;

H = 3 – высота помещения, м.

Тогда высота подвеса светильников составит

$$h_{\text{расч}} = H - \left(h_{\text{рабпов}} + h_{\text{свеса}}\right) = 3 - (0{,}35 + 1) = 1{,}65 \text{ м},$$

Схема расположения светильников и световых проемов представлена на рисунке 5.3

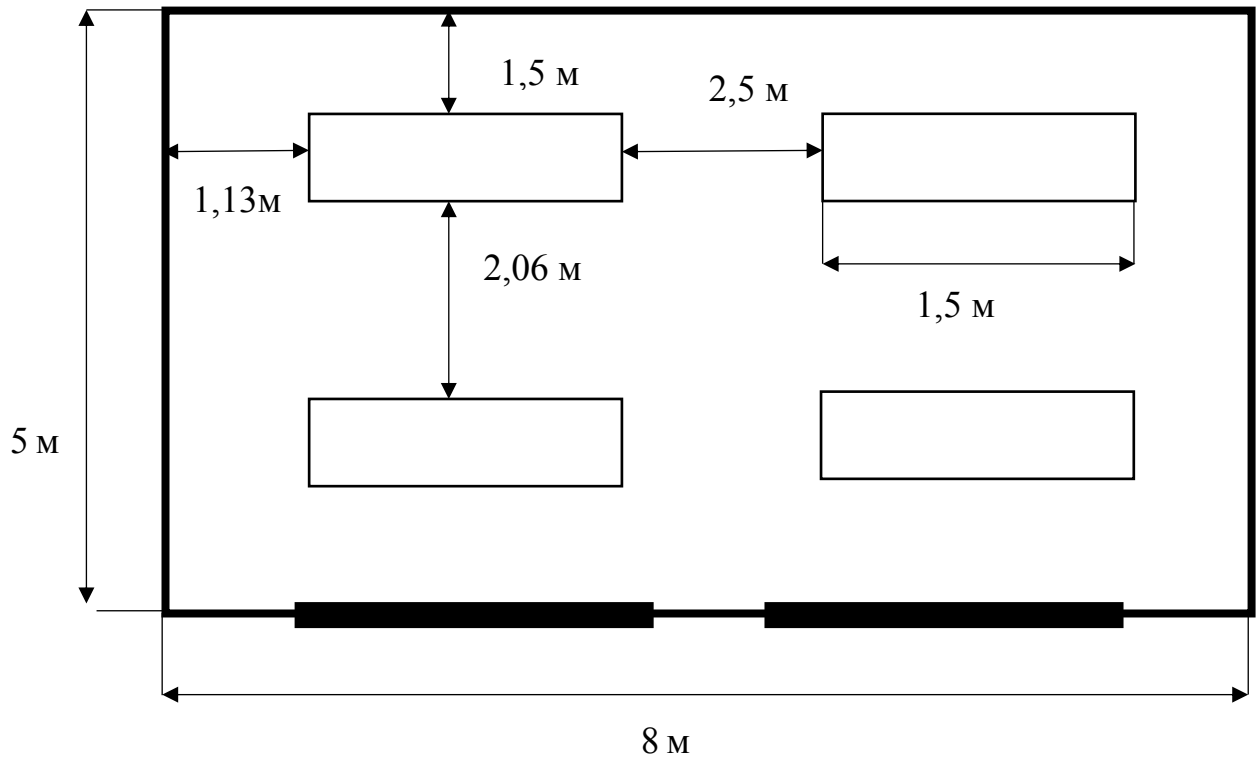


Рисунок 5.3 Расположение светильников и световых проемов в помещении

Вывод: в данной главе был проведен анализ оптимальных условий труда для выполнения исследования по теме дипломного проекта. На основе проведенных вычислений была проведена реконструкция искусственного освещения. В частности было принято решение увеличить количество светильников с двух до четырех, а так же поменять старые люминесцентные лампы по 55 Вт со световым потоком 3020 лм на новые люминесцентные лампы по 85 Вт со световым потоком 3600лм (тип светильника TLPL236)

6 Экономическая часть

6.1 Технико - экономическое обоснование

Тема данной дипломной работы рассматривает внутренние угрозы кибер безопасности. Целью является уменьшение количества утечек конфиденциальной информации.

В данной главе будут рассчитаны все необходимые затраты и расходы в процессе выполнения дипломной работы такие как расходы на электроэнергию, приобретение необходимых ресурсов, оплаты труда, а также на затраты амортизационных отчислений. [17]

6.2 Расчет трудоемкости выполнения работы

Для того чтобы определить точный расчет трудоемкости выполнения дипломной работы был составлен перечень всех этапов и стадий работ, которые должны быть выполнены. Трудоемкость деятельности обусловливалась в соответствии с общепризнанным меркам периода в осуществление расчетов, рассмотрения и проведение исследования. В таблице 6.1 представлена следующая модель расчета трудоемкости выполнения дипломной работы.

Таблица 6.1 – Пошаговое распределение работ и оценка их трудоемкости

Этапы разработки ПП	Виды работ	Трудоемкость разработки, чел. х ч.
1 этап	Изучение задания, постановка целей и задач	10
2 этап	Поиск, ознакомление и изучение литературы по теме дипломной работы	50
3 этап	Поиск и анализ угроз информационной безопасности	40
5 этап	Поиск и анализ программного обеспечения	25
6 этап	Установка и настройка среды для проведения работы	15
7 этап	Установка операционных систем, программного обеспечения и утилит	20
8 этап	Реализация моделирования утечек	60
9 этап	Оформление итогового отчета	30
ИТОГО: трудоемкость выполнения проекта		250

В результате (250ч/8ч) для выполнения работы потребуется 31 рабочий день.

6.3 Расчет всевозможных затрат на выполнение дипломной работы

Определение затрат на выполнение дипломной работы производится на основе следующих элементов:

– вычисление материальных затрат;
– вычисление затрат на оплату труда;
– расчет социального налога;
– вычисление амортизационных отчислений;
– расчет на прочие затраты.

Вычисление материальных затрат заключается в проведении подсчета всех расходов на необходимое оборудование и программное обеспечение, которое нужно для проведения исследования по теме дипломной работы.

Затраты на облачное хранилище не будут рассчитываться потому как она является бесплатным. Расчет затрат на все необходимые ресурсы, а также операционную систему и программное обеспечение производится по форме, приведенной в таблицах 6.2., 6.3

Таблица 6.2 – Затраты на оборудование и ПО, необходимые для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	Acer Aspire E5–575G	Шт.	1	219 900	219 990,00
Принтер	Canon LBP–6030B A4	Шт.	1	69 990	69 990,00
Компьютерная мышь	Hyperx Pulsefire FPS	Шт.	1	20 990	20 990,00
Модем	Wi–Fi модем Tenda D305	Шт.	1	13 000	13 000,00
ПО	JETLOGGER	Шт.	1	16 810	16 810,00
ПО	Microsoft Office	Шт.	1	39 990	39 990,00
ПО	VMware Workstation 15 Pro	Шт.	1	59 990	59 990,00
Итого:					440 760,00

Таблица 6.3 – Затраты на материальные ресурсы

Наименование материала	Количество	Ед. измерения	Цена за ед. в тенге	Сумма в тенге
Блокнот	1	Шт.	850	850,00
Ручки	5	Уп.	150	750,00
Бумага А4	1	Уп.	1286	1286,00
Картридж для принтера	3	Шт.	5990	17970,00
Степлер	5	Шт.	350	1750,00
Скобы для степлера	1	Уп.	65	65,00
Файл–вкладыш	20	Уп.	685	13700,00
Органайзер	2	Шт.	450	900,00
Папки регистраторы	10	Шт.	400	4000,00
Итого				41 270,00

Общая сумма расходов на материальные средства (Зм) определяется в соответствии с формулой (6.1)

$$Зм = \sum Pi \times Цi, \quad (6.1)$$

где P_i – расход i–го вида материального ресурса, натуральные единицы;

$Ц_i$ – цена за единицу i–го вида материального ресурса, тг;

i – вид материального ресурса;

n – количество видов материальных ресурсов.

Зм = 219990 + 69990 + 20990 + 18990 + 16810 + 39990 + 59990 + 850+ 750 + 1286 + 17970 + 1750 + 65 + 13700 + 900 + 4000 = 482 031,00 (тенге)

В результате расходы на материальные нужды дипломной работы составят 482 031,00 тенге.

Вычисление расходов на затраты электроэнергии необходимо так как в процессе выполнения дипломной работы все время используется электрооборудование такое как ноутбук, модем, принтер и т.д. Расчет затрат на электроэнергию содержит в себе затраты электроэнергии на оборудование и дополнительные нужды.

Согласно данным из таблицы 6.1 время работы оборудования составляет 250 часов для ноутбука и модема. Для принтера длительность работы берется число равное 50 часам так как отсутствует необходимость постоянного его использования.

$$Э = З_{эл.эн.\ обор} + З_{доп.нуж}, \quad (6.2)$$

где $З_{эл.эн.обор}$ – затраты на электроэнергию оборудования;

$З_{доп.нуж.}$ – затраты электроэнергии на дополнительные нужды.

Расходы электроэнергии на оборудование определяются в соответствие с формулой (6.3)

$$З_{эл.эн.обор} = \sum W \times К_{исп.} \times S \times T, \quad (6.3)$$

где W – потребляемая мощность, Вт;

$К_{исп}$ – коэффициент использования ($К_{исп}$ = 0,7 – 0,9);

T – время работы;

S – тариф (1кВт/ч = 18,32 тг).

В таблице 6.4 записаны следующие расчеты затрат на электроэнергию.

Таблица 6.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/ кВтч	Сумма, тг
Ноутбук	0,6	0,7	250	18,32	1923,6
Модем	0,08	0,9	250	18,32	329,76
Принтер	0,5	0,9	50	18,32	409,5
Освещение	0,3	0,7	250	18,32	961,8
Итого	3624,66				

$$З_{эл.эн.обор.} = 1923,6 + 329,76 + 409,5 + 961,8 = 3624,66 \text{ (тенге)}$$

Расходы на дополнительные потребности принимаются согласно укрупненному показателю в объеме 5% от расходов на оборудование:

$$З_{доп.нуж.} = 5\% \times З_{эл.эн.обор.}, \quad (6.4)$$

Затраты на дополнительные потребности определяется в соответствие с формулой (6.4):

$$З_{доп.нуж} = 0,05 \times 3624,66 = 181,233 \text{ (тенге)}$$

Таким образом итоговые расходы в электроэнергию составляют:

$$Э = 3624,66 + 181,233 = 3805,893 \text{ (тенге)}$$

Над выполнением исследования работают два человека:

- руководитель проекта, который отвечает за составление плана работы и контролирует его выполнение, а также отвечает за правильность выполнения работы и поддержку;
- программист–исследователь, занимающийся исследованием, изучением ПО, экспериментированием, составлением и оформлением отчета.

Общая сумма затраты на оплату труда (Зтр) высчитывается по следующей формуле (6.5)

$$З_{тр} = \sum ЧС_i \times Т_i, \quad (6.5)$$

где ЧСi – часовая ставка i–го работника, тенге;
Ti – трудоемкость разработки модели, чел.×ч;
i – категория работника;
n – количество работников, занятых разработкой ПП.

В процессе выполнения работы, сотрудники, выполняющие свою работу, задействованы неравноценно, поэтому есть необходимость в вычислении часовой ставки сотрудника, а после и общего объема заработной платы.

Часовая ставка сотрудника рассчитывается по формуле (6.6)

$$ЧСi = ЗПi / ФРВi, \quad (6.6)$$

где ЗПi – месячная заработная плата i–го работника, тенге;
ФРВi – месячный фонд рабочего времени i–го работника, час.

Месячная заработная плата сотрудников: руководитель – 280 000,00 тенге, программист–исследователь – 160 000,00 тенге. ФРВ работника составляет 176 часов, так как в месяце 22 рабочих дня, а рабочий день длится 8 часов.

$$ЧС_i = 280\,000 / 176 = 1600 \text{ тг/ч}$$

$$ЧС_i = 160\,000 / 176 = 909 \text{ тг/ч}$$

Часовая ставка научного руководителя составляет 1600 (тг/ч), трудоемкость разработки – 100 ч., так как руководитель проекта участвует

только на первых трех этапах. Часовая ставка разработчика составляет 909 (тг/ч), трудоемкость разработки – 250 часов.

Следовательно, общая сумма расходов на оплату труда согласно формуле 6.5 будет составлять:

$$З_{тр} = 1600 \times 100 + 909 \times 250 = 160\,000 + 227\,250 = 387\,250 \text{ (тенге)}$$

Результаты расчета затрат на оплату труда показаны в таблице 6.5.

Таблица 6.5 – Расчёт заработной платы сотрудников

Категория работника	Квалификация	Трудоемкость разработки, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель проекта	Инженер проектировщик	100	1600	160 000
Программист	Исследователь	250	909	227 250
Итого				387 250

Социальный налог согласно Налоговому кодексу Республики Казахстан составляет 9,5% от ФОТ (фонда оплаты труда). Следует отметить, что пенсионные отчисления не облагаются социальным налогом.

$$С_н = (ФОТ - ПО) \times 0{,}095, \qquad (6.7)$$

где ПО – отчисления в пенсионный фонд, 10% от ФОТ.

Социальный налог рассчитываем по формуле (6.7):

$$ПО = 387\,250 \times 0{,}1 = 38\,725 \text{ тенге;}$$

$$С_н = (387\,250 - 38\,725) \times 0{,}095 = 33\,109{,}875 \text{ тенге}$$

Результаты вычисления затрат на социальный налог представлены в таблице 6.6.

Таблица 6.6 – Затраты на социальный налог

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель проекта	1	160 000	16 000	13 680
Студент	1	227 250	22 725	19 429,875
Итого				33 109,875

Годовые нормы амортизации ОФ берутся согласно налоговому кодексу РК либо формируются, отталкиваясь из вероятного срока полезного использования ОФ. Амортизация основных фондов определяется согласно формуле (6.8)

$$А_г = С_{об} \times Н_а / 100, \quad (6.8)$$

где, $С_{об}$ – стоимость оборудования;

$Н_а$ – норма амортизации (норма амортизация = 25);

По формуле 6.8 рассчитаем необходимую сумму амортизационных отчислений за год для ноутбука:

$$А_г = 219\ 990 \times 25 / 100 = 54\ 997 \text{ тенге}$$

Рассчитаем сумму амортизации за период разработки:

$$А_г = 54\ 997 \times 31 / 365 = 4\ 670{,}978$$

Подобным методом рассчитаем сумму амортизации для прочего оборудования. Результаты расчетов приведены в таблице 6.7

Таблица 6.7 – Амортизация основных фондов (ОФ)

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Ноутбук	219 990	25	54 997	4 670,97
Принтер	69 990	15	10 498,5	891,32
Компьютерная мышь	20 990	15	3 148,5	267,30

Продолжение таблицы 6.7

Модем	13 000	15	2 848,5	241,83
ПО JETLOGGER	16 810	15	2 521,5	214,07
ПО Microsoft Office	39 990	15	5 998,5	509,27
ПО VMware Workstation Pro	59 990	15	8 998,5	763,97
ИТОГО			89 011,3	7 558,7

6.4 Смета расходов и затрат на выполнение дипломной работы

На основе выполненных расчетов оформляется смета расходов на выполнение дипломной работы. Смета представляется в виде таблицы 6.8, либо в виде рисунка 6.1.

Таблица 6.8 – Смета затрат на выполнение дипломной работы

Наименование расходов	Сумма, тг
Затраты на оборудование и ПО	440 760
Затраты на материальные ресурсы	41 270
Затраты на оплату труда	387 250
Социальные налоги	33 109,875
Затраты на электроэнергию	3624,66
Амортизация основных фондов	7 558,7
Итого	913 573,235

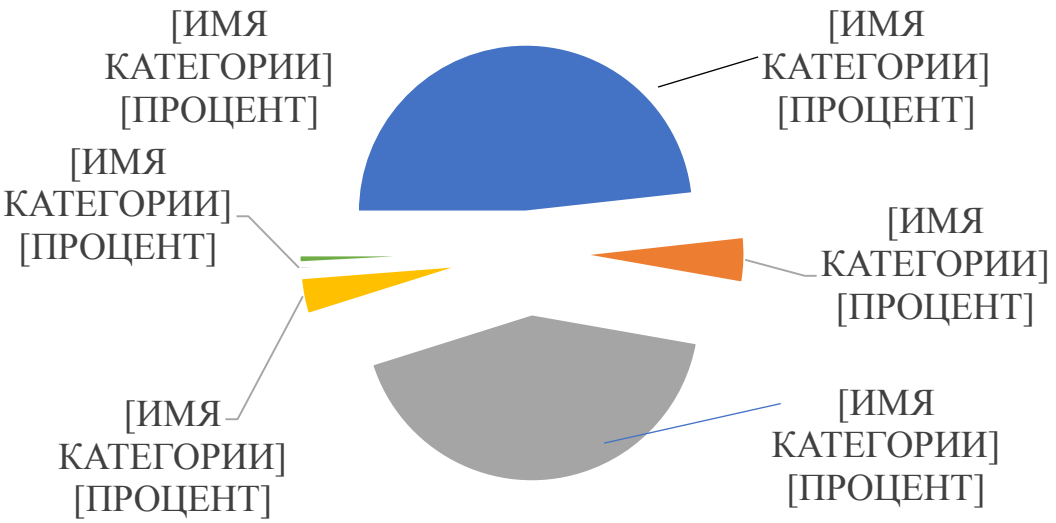


Рисунок 6.1 – Смета затрат

6.5 Определение возможной (договорной) цены программного продукта

Величина возможной (договорной) цены программного продукта устанавливается на основе эффективности, качества и сроков её выполнения на уровне, отвечающем экономическим интересам заказчика (потребителя) и исполнителя. Договорная цена ЦД для прикладных программных продуктов рассчитывается по формуле (6.9)

$$ЦД=ЗНИР(1+Р100) \quad (6.9)$$

где ЗНИР– затраты на разработку ПП, тг;

Р – средний уровень рентабельности ПП. % (принимается в размере 20%).

ЦД = 913 573,23 × (1 + 20/100) = 913 573,23 × 1,2 = 1 096 287,88 тенге
Значение прибыли составляет 182 714,65 тенге

Далее определяется цена реализации с учетом налога на добавленную стоимость (НДС), ставка (НДС) устанавливается законодательно. Налоговым Кодексом РК. На 2019 год ставка НДС установлена в размере 12%.

Цена реализации с учетом НДС рассчитывается по формуле:

$$Цр = ЦД + ЦД\times НДС \quad (6.10)$$

$$1\ 096\ 287{,}88+ (1\ 096\ 287{,}88\times 0{,}12) = 1\ 096\ 287{,}88+ 131\ 554{,}54 =$$

$$= 1\ 227\ 842{,}43 \text{ тенге}$$

Вывод: в данной главе были вычислены затраты на приобретение всего необходимого оборудования, а также операционных систем и программного обеспечения для реализации исследования по теме дипломной работы. Кроме того, был произведен расчет заработной платы как технического руководителя, так и программиста, а также их пенсионные отчисления включая социальный налог. Так как в ходе выполнения работы была необходимость использования оборудования, которое потребляет электроэнергию, было произведено вычисление затрат на электроэнергию. В результате подводя итог, затраты, которые необходимы для выполнения дипломной работы составляют 913 573,23 тенге. Цена реализации с учетом НДС соавляет 1 227 842,43 тенге. Прибыль: 182 714,65 тенге.

Заключение

Во время подготовки дипломной работы было изучено множество существующих методов социальной инженерии. Предложена общая классификация угроз для организаций.

Согласно статистике, 70% несанкционированного доступа к информации генерируется с помощью социальной инженерии, которая в свою очередь использует человеческий фактор и сотрудников, которые не соблюдают правила безопасности. Подразделениями в организации, занимающимися безопасностью и кадровой безопасностью, являются технический отдел и отдел кадров. Они должны находиться в тесном и постоянном взаимодействии.

Каждая компания сталкивается с трудным выбором между повышенной безопасностью и производительностью сотрудников, что приводит к тому, что некоторые сотрудники игнорируют правила безопасности, не понимая, насколько важно защитить целостность конфиденциальной информации в своей организации.

Чтобы уменьшить эти риски, в этой последней квалификационной работе был разработан метод борьбы с социальной инженерией, описывающий теоретические аспекты социальной инженерии, методы, позволяющие воздействовать на работников организации и методы, которые сотрудники должны придерживаться для того, чтобы: уменьшить реализацию угрозы социальных инженеров.

Комплекс всех мер по противодействию социальному инжинирингу способствует укреплению организаций, их стабильности и безопасности, экономическому развитию, внося тем самым лепту в профилактику экономических преступлений и нарушений, укрепляя экономику на всех уровнях.

Список литературы

1 Алавердов А. Р. Кадровая безопасность современного банка: стратегия и тактика управления. – М.: Маркет ДС, 2004. – 82 с.

2 Алавердов А.Р. Управление кадровой безопасностью организации – М.: Маркет ДС, 2010. – 176 с.

3 Доля А. Саботаж в корпоративной среде. URL: http://citforum.ru/security/articles/sabotage/ (дата обращения: 02.02.2019).

4 Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: Учеб. пособие. – М.: ФОРУМ, 2009. – 256 с.

5 Мельникова, Е. И. Формы утечки информации, составляющей коммерческую тайну, и управление персоналом предприятия в целях обеспечения информационной безопасности. URL: http://center–bereg.ru/h1088.html (дата обращения: 12.02.2019).

6 Скиба В., Курбатов В. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Издательство Питер, 2008. – 320 с.

7 Кодексы Республики Казахстан URL:https://kodeksy-kz.com/ka/ob_administrativnyh_pravonarusheniyah/79.htm (дата обращения:10.03.19)

8 Скляренко А. Угрозы конфиденциальности информации, связанные с персоналом – СПб.: БХВ–Петербург, 2010. – 92 с.

9 Андреева Г. М. Социальная психология: учебник для вузов – М.: ЭЛИТ, 2003. – 270 с.

10 Касперски К. Секретное оружие социальной инженерии URL: https://www.osp.ru/lan/2002/09/136546 (дата обращения: 12.03.2019).

11 Кузнецов М. В. Социальная инженерия и социальные хакеры: учеб. метод. пособие. – СПб.: БХВ–Петербург, 2010. – 368 с.

12 Митник К. Д. Искусство обмана: Учеб. пособие – NYC.: Wiley Books. 2008. – 273 с.

13 Шейнов В. П. Искусство управлять людьми: Учеб. пособие. – Мн.: Харвест, 2005. – 512 с.

14 Информационная безопасность. URL: https://bookucheba.com/informatsionnaya–bezopasnost_1280/issledovanie–sistemnyih–logov–45416.html (дата обращения: 25.03.2019).

15 И.Ф. Мазалов, К.Г. Мустафин, Е.М. Тыщенко, М.А. Сералиева Методические указания по выполнению РГР для студентов специальности 5В073100–БЖ. – Алматы: АУЭС, 2015. – 38 с.

16 СНиП РК 2.04 – 05 – 2002. Естественное и искусственное освещение. Общие требования. Астана: Стройиздат, 2002. – 15 с.

17 Аманжолова К. Б., Алибаева С. А. Экономика предприятий телекоммуникаций: Учебное пособие. – Алматы: АИЭС, 2003. – 70 с.