автономная некоммерческая организация
«Аналитический центр при Правительстве Российской Федерации»

УТВЕРЖДАЮ:
Заместитель руководителя
автономной некоммерческой организации
«Аналитический центр при
Правительстве Российской Федерации»

_____ Н.Д. Беликов

8 декабря 2020 г

ДОКУМЕНТАЦИЯ

о запросе цен в электронной форме на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

г. Москва, 2020 г.

Автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации» приглашает юридических и физических лиц, в том числе индивидуальных предпринимателей, которые соответствуют требованиям, установленным настоящей Документацией, принять участие в запросе цен в электронной форме (далее – запрос цен) на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

1. Законодательное регулирование

Настоящая Документация подготовлена на основе Гражданского кодекса Российской Федерации и Положения о закупочной деятельности автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (далее – Положение), утвержденного решением наблюдательного совета автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (протокол № 1 от 24 марта 2015 года, с изменениями, утвержденными протоколом № 7 от 20 июня 2017 года). В части, прямо не урегулированной законодательством Российской Федерации, проведение запроса цен регулируется настоящей Документацией и Положением.

2. Основные термины

Документация – комплект документов, содержащий всю необходимую информацию о предмете запроса цен, условиях исполнения договора, требованиях к Участникам, а также об условиях проведения запроса цен.

Заказчик – автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации» (Аналитический центр при Правительстве Российской Федерации).

Запрос цен – непродолжительная (до 7 календарных дней) процедура формального запроса технико-коммерческих предложений с выбором лучшего предложения по лучшей цене и без обязанности Заказчика заключить договор по результатам такой закупочной процедуры.

Заявка – комплект документов Участника, подтверждающих правоспособность и квалификацию Участника и содержащих предложение об условиях исполнения договора на поставку Продукции, являющейся предметом запроса цен.

Комиссия по закупкам, Комиссия – коллегиальный орган, создаваемый Заказчиком для выбора Поставщика путем проведения закупочных процедур с целью заключения договора.

Лот – часть закупаемой продукции, на которую в соответствии с извещением и Документацией допускается подача отдельной Заявки и заключение отдельного договора по итогам запроса цен.

Начальная (максимальная) цена договора – предельная цена Продукции, являющейся предметом запроса цен, рассчитанная Заказчиком в установленном порядке или определенная Заказчиком по результатам изучения конъюнктуры рынка.

Продукция, Предмет закупки – товары, работы или услуги, приобретаемые для нужд Заказчика.

Размещение закупки – публикация на электронной торговой площадке и сайте Заказчика информации о проведении Заказчиком закупочной процедуры.

Сайт Заказчика – сайт в информационно-телекоммуникационной сети Интернет, где размещается информация о проведении открытых закупочных процедур на приобретение Продукции для нужд Заказчика (http://ac.gov.ru).

Участник – участник запроса цен – потенциальный Поставщик, претендующий на поставку Продукции для нужд Заказчика.

Электронная площадка – электронная торговая площадка OTC-tender (www.otc-tender.ru).

3. Общие сведения о процедуре запроса цен

Запрос цен проводится в соответствии с законодательством Российской Федерации, но не является разновидностью торгов и не подпадает под регулирование статьями 447-449 части первой Гражданского кодекса Российской Федерации. Запрос цен также не является публичным конкурсом и не регулируется статьями 1057-1061 части второй Гражданского кодекса Российской

Федерации. Таким образом, данная процедура не накладывает на Заказчика соответствующего объема гражданско-правовых обязательств.

Участники самостоятельно несут все расходы, связанные с участием в запросе цен, подготовкой и подачей Заявок; Заказчик по этим расходам не отвечает и не имеет обязательств, независимо от хода и результатов данного запроса цен.

Заказчик вправе отклонить Заявку, если он установит, что Участник прямо или косвенно дал, согласился дать или предложил работнику Заказчика вознаграждение в любой форме: работу, услугу, какую-либо ценность в качестве стимула, который может повлиять на принятие Комиссией по закупкам решения по определению победителя.

Заказчик вправе отклонить Заявки Участников, заключивших между собой какое-либо соглашение с целью повлиять на определение победителя запроса цен.

3.1. Используемый способ закупки: запрос цен в электронной форме.

3.2. Наименование Заказчика: автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации».

Место нахождения: 107078, Москва, проспект Академика Сахарова, д. 12.

Почтовый адрес: 107078, Москва, проспект Академика Сахарова, д. 12.

Адрес электронной почты: torgi@ac.gov.ru.

Номер контактного телефона: +7 (916) 209 67 30.

Ответственное должностное лицо Заказчика: Чернявский Константин Александрович.

3.3. Предмет закупки: предоставление неисключительных прав на использование программы для ЭВМ (далее – неисключительные права или неисключительная лицензия)- Программный продукт «DLP система Falcon Gaze Secure Tower» (далее – Продукт) для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

3.4. Место и сроки поставки Продукции:

Место поставки Продукции: г. Москва, проспект Академика Сахарова, дом 12.

Сроки поставки Продукции: Срок передачи Продукта: в течение 7 (Семи) рабочих дней с даты заключения договора.

4. Сведения о начальной (максимальной) цене договора:

9 121 800,00 (Девять миллионов сто двадцать одна тысяча восемьсот) рублей 00 копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

5. Форма, сроки и условия оплаты:

Оплата за предоставление неисключительных прав на использование Продукта осуществляется Заказчиком по факту предоставления неисключительных прав на использование Продукта в течение 10 (Десяти) рабочих дней с даты получения счета, выставленного на основании подписанного Сторонами акта передачи прав.

6. Порядок формирования цены договора:

Цена договора включает в себя все обязательные платежи и расходы, связанные с исполнением договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

7. Порядок, место, время начала и окончания срока подачи Заявок

Запрос цен проводится на Электронной площадке (www.otc-tender.ru) в порядке, установленном регламентом данной Электронной площадки (www.otc-tender.ru) в соответствии с условиями и требованиями Документации.

Для участия в запросе цен Участник должен быть зарегистрированным на указанной Электронной площадке (www.otc-tender.ru), в том числе, получить аккредитацию участника Электронной площадки (www.otc-tender.ru) в соответствии с правилами, условиями и порядком регистрации, аккредитации, установленными данной Электронной площадкой (www.otc-tender.ru).

Заявка на участие в запросе цен подается Участником закупки в электронной форме.

Прием заявок осуществляется на Электронной площадке (www.otc-tender.ru).

Дата начала подачи Заявок: в день размещения документации на сайтах www.ac.gov.ru и www.otc-tender.ru.

Дата окончания срока подачи Заявок: 11 декабря 2020 года в 15.00 (мск).

Место подачи Заявок: Электронная площадка (www.otc-tender.ru)

8. Требования к участникам закупки и перечень документов, представляемых участниками закупки для подтверждения их соответствия установленным требованиям:

8.1. Участник должен соответствовать требованиям, предъявляемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставки Продукции, являющейся предметом Закупки, в том числе:

а) быть правомочным заключать договор;

б) обладать необходимыми лицензиями или свидетельствами для поставки Продукции, подлежащей лицензированию (регулированию) в соответствии с действующим законодательством Российской Федерации и являющейся предметом заключаемого договора;

в) обладать необходимыми сертификатами на Продукцию, являющуюся предметом заключаемого договора, в соответствии с действующим законодательством Российской Федерации;

г) не находиться в процессе ликвидации (для юридического лица) или банкротства;

д) не являться юридическим или физическим лицом, на имущество которого наложен арест по решению суда, административного органа и/или экономическая деятельность которого приостановлена;

е) не иметь за прошедший календарный год задолженности по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды, размер которой превышает двадцать пять процентов балансовой стоимости активов, определяемой по данным бухгалтерской отчетности за последний завершенный отчетный период;

ж) обладать профессиональной компетентностью, финансовыми и трудовыми (кадровыми) ресурсами, оборудованием и другими материальными возможностями, надежностью, опытом и репутацией, необходимыми для исполнения договора на поставку Продукции;

з) руководитель и главный бухгалтер юридического лица, являющегося Участником, не должны иметь непогашенной или неснятой судимости в сфере экономики;

и) Участник не должен быть включен в реестр недобросовестных поставщиков, предусмотренный Федеральным законом от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а также в реестр недобросовестных поставщиков Аналитического центра при Правительстве Российской Федерации.

к) Участник закупки - юридическое лицо, которое в течение двух лет до момента подачи заявки на участие в закупке не было привлечено к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях.

8.2. Заявка на участие должна содержать:

а) фирменное наименование (наименование), сведения об организационно-правовой форме, о месте нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные, сведения о месте жительства (для физического лица), номер контактного телефона;

б) копии учредительных документов Участника (для юридических лиц);

в) копии документов о государственной регистрации юридического лица или физического лица в качестве индивидуального предпринимателя в соответствии с законодательством Российской Федерации; для физического лица - копии документов, удостоверяющих личность; надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица или государственной регистрации

физического лица в качестве индивидуального предпринимателя в соответствии с законодательством соответствующего государства (для иностранного лица);

г) копии свидетельства о постановке на учет в налоговом органе (для юридических и физических лиц), уведомления о постановке на учет в налоговом органе (для индивидуальных предпринимателей);

д) полученные не ранее чем за шесть месяцев до дня размещения на сайте Заказчика Извещения о проведении запроса цен:

- выписку или нотариально заверенную копию выписки из единого государственного реестра юридических лиц (для юридического лица);

- выписку или нотариально заверенную копию выписки из единого государственного реестра индивидуальных предпринимателей (для индивидуального предпринимателя);

е) копию документа, подтверждающего полномочия лица на осуществление действий от имени Участника - юридического лица (копия решения о назначении или об избрании, или приказа о назначении физического лица на должность, в соответствии с которым такое физическое лицо обладает правом действовать от имени Участника без доверенности (далее по тексту - руководитель). В случае, если от имени Участника действует иное лицо, Заявка на участие в запросе цен должна содержать также доверенность на осуществление действий от имени Участника, заверенную печатью Участника и подписанную руководителем Участника (для юридических лиц) или уполномоченным этим руководителем лицом, либо нотариально заверенную копию такой доверенности. В случае если указанная доверенность подписана лицом, уполномоченным руководителем Участника, Заявка на участие в запросе цен должна содержать также документ, подтверждающий полномочия такого лица;

ж) копию документа, удостоверяющего личность индивидуального предпринимателя или лица, действующего от имени юридического лица (индивидуального предпринимателя);

з) решение об одобрении или о совершении крупной сделки либо копию такого решения в случае, если для Участника поставка товаров, выполнение работ, оказание услуг, являющихся предметом договора, или внесение денежных средств в качестве обеспечения исполнения договора, обеспечения гарантийных обязательств являются крупной сделкой. В случае, если для данного Участника поставка товаров, выполнение работ, оказание услуг, являющиеся предметом договора, или внесение денежных средств в качестве обеспечения не являются крупной сделкой, Участник представляет соответствующее письмо;

и) копии документов, подтверждающих соответствие Участника требованиям, устанавливаемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим выполнение работ, оказание услуг, поставку товара, являющихся предметом запроса цен (копии действующих лицензий по предмету запроса цен, допусков, членства в саморегулируемых общественных организациях, декларация о соответствии или иные документы);

к) копию уведомления о возможности применения Участником упрощенной системы налогообложения (для Участников, применяющих ее);

л) копии документов, подтверждающих обладание Участниками исключительными правами на объекты интеллектуальной собственности, если в связи с исполнением договора Заказчик приобретает исключительные права на объекты интеллектуальной собственности;

м) справка (или копия справки) налогового органа об исполнении Участником обязанности по уплате налогов, сборов, пеней и налоговых санкций и отсутствии задолженности;

н) оригиналы согласия на обработку персональных данных руководителя (лица осуществляющего действия от имени Участника), индивидуального предпринимателя или физического лица (Приложение № 3 к Документации)

о) Заявку (Приложение № 2 к Документации);

К Заявке в обязательном порядке должны быть приложены:

- предложение о функциональных характеристиках (потребительских свойствах) и качественных характеристиках. (Приложение № 1 к Заявке);

- копия, действующего на момент подачи заявки, договора, подтверждающего наличие соответствующих полномочий Участника от правообладателя прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower».

- анкета Участника (Приложение № 2 к Заявке).

Все предоставленные документы должны быть в виде электронных документов в формате *.doc, *.docx или *.pdf и подписаны электронной подписью лица, имеющего право действовать от имени Участника.

9. Порядок предоставления документации о закупке: Документация доступна для ознакомления и скачивания на сайте Заказчика (www.ac.gov.ru) и сайте Электронной площадки (www.otc-tender.ru) без взимания платы.

10. Формы, порядок, дата начала и дата окончания срока предоставления Участникам Закупки разъяснений положений Документации, порядок внесения изменений:

10.1. Любой Участник вправе направить Заказчику запрос о разъяснении положений Документации:

а) через Электронную площадку (www.otc-tender.ru);

б) в письменной форме на почтовый адрес Заказчика, указанный в п. 3.2 Документации.

10.2. Датой начала срока предоставления разъяснений положений Документации является 1 (Первый) рабочий день с даты размещения Документации. Датой окончания срока предоставления разъяснений положений Документации является рабочий день, предшествующий дню окончания приема заявок на участие в закупке.

10.3. Заказчик после получения запроса от Участника в течение 1 (Одного) рабочего дня осуществляет подготовку разъяснений и размещает их на Электронной площадке. Разъяснение положений Документации не должно изменять Документацию.

Заказчик вправе не отвечать на запрос Участника, если он поступил позднее, чем за 3 (Три) рабочих дня до срока окончания подачи Заявок.

10.4. Заказчик по собственной инициативе или на основании запроса Участника вправе принять решение о внесении изменений в Документацию о проведении запроса цен и извещение о проведении закупки. В зависимости от характера изменений, внесенных в Документацию о проведении запроса цен, по решению Заказчика может быть продлен срок окончания подачи заявок.

10.5. Изменения, вносимые в извещение о закупке и в Документацию о проведении запроса цен в электронной форме, размещаются Заказчиком на сайте Заказчика (www.ac.gov.ru) и сайте Электронной площадки (www.otc-tender.ru)в течение 1 (Одного) рабочего дня со дня принятия решения о внесении изменений.

10.6. Участники, получившие Документацию о проведении запроса цен в электронной форме с сайта Заказчика (www.ac.gov.ru) или сайта Электронной площадки (www.otc-tender.ru), должны самостоятельно отслеживать изменения Извещения и Документации о проведении запроса цен в электронной форме. Заказчик не несет ответственности за несвоевременное получение Участниками информации с сайта Заказчика (www.ac.gov.ru) или сайта Электронной площадки (www.otc-tender.ru).».

11. Место, порядок, дата и время открытия доступа к Заявкам на участие в закупке:

Открытие доступа к Заявкам на участие в запросе цен осуществляется 11 декабря 2020 года в 15.00 (мск).

12. Критерии оценки и сопоставления Заявок на участие в Закупке.

Оценка заявок, поданных Участниками, производится по единственному критерию – «цена договора».

13. Порядок оценки и сопоставления Заявок

Комиссия по закупкам в срок, указанный в Документации, осуществляет оценку и сопоставление Заявок на участие в запросе цен, признанных соответствующими требованиям Документации.

Оценка заявок осуществляется в соответствии с критерием «цена договора».

Лучшей признается Заявка Участника, в которой предложена наименьшая цена договора.

В случае если Участник освобождается от исполнения обязанности налогоплательщика НДС, либо Участник не является налогоплательщиком НДС то цена, предложенная таким Участником в Заявке, не должна превышать установленную начальную (максимальную) цену без учета НДС.

При этом в указанном случае на стадии оценки и сопоставления Заявок для целей сравнения ценовые предложения всех Участников также учитываются без НДС.

14. Место и дата рассмотрения Заявок и подведения итогов закупки.

Рассмотрение Заявок и подведение итогов закупки осуществляются 11 декабря 2020 года по адресу: г. Москва, проспект Академика Сахарова, дом 12.

15. Условия допуска к участию в закупке:

15.1. Предложение участника закупки не должно превышать начальной (максимальной) цены договора, установленной Документацией.

15.2. Если Участником представлен не полный комплект документов или представленные документы оформлены с нарушением требований, установленных подпунктом 8.2. Документации и Приложением № 2 к Документации, то Комиссия по закупкам расценивает это как существенное несоответствие Заявки на участие в запросе цен требованиям, установленным Документацией, и данная Заявка не допускается к участию в запросе цен.

15.3. Результаты рассмотрения Заявок фиксируются в протоколе рассмотрения Заявок на участие в запросе цен. Протокол должен содержать сведения об участниках процедуры закупки, подавших Заявки на участие в запросе цен, решение о допуске участника процедуры закупки к участию в запросе цен и о признании его участником запроса цен или об отказе в допуске участнику процедуры закупки в участии в запросе цен с указанием положений Документации о проведении запроса цен, которым не соответствует Участник процедуры закупки или Заявка такого участника.

15.4. Протокол должен быть составлен и подписан членами Комиссии по закупкам не позднее 3 (Трех) дней с даты окончания рассмотрения Заявок, установленной Документацией о проведении запроса цен.

15.5. По решению Комиссии по закупкам вскрытие Заявок, рассмотрение Заявок Участников и принятие решения о допуске (отказе в допуске) Участников к участию в запросе цен может оформляться одним протоколом.

15.6. Протоколы, составленные в ходе проведения закупки, Заявки на участие в закупке, документация, изменения, внесенные в документацию, разъяснения положений документации подлежат хранению не менее трех лет.

16. Ограничение участия в определении поставщика: не предусмотрено.

17. Размер обеспечения исполнения договора: не установлен.

18. Сведения о предоставлении преференций: не установлены.

19. Содержание, форма, оформление и состав Заявки на участие в закупке:

Заявка на участие в запросе цен, оформленная согласно Приложению № 2 к Документации, подается Заказчику в электронной форме на сайте Электронной площадки (www.otc-tender.ru).

20. Преддоговорные переговоры.

20.1. Между Заказчиком и Участником, с которым заключается договор, могут проводиться преддоговорные переговоры (с оформлением протокола таких переговоров и его подписанием обеими сторонами), направленные на уточнение условий договора.

20.2. Допускается проводить преддоговорные переговоры по следующим вопросам:

а) по снижению цены договора и (если применимо) цен отдельных видов товаров, расценок на отдельные виды работ (услуг) без уменьшения количества товаров, объема работ, услуг;

б) по увеличению объемов Продукции без увеличения цен (расценок);

в) по сокращению сроков выполнения договора (его отдельных этапов) и (или) улучшению условий для Заказчика: отмена аванса, улучшение технических характеристик продукции и т.д.

г) по уточнению условий договора, которые не были зафиксированы в проекте договора, Документации и заявке Участника, с которым заключается договор.

20.3. Запрещаются преддоговорные переговоры, направленные на изменение условий заключаемого договора в пользу Участника, с которым заключается договор.

21. Заключение договора

21.1. Заказчик в течение 2 (Двух) рабочих дней со дня размещения протокола оценки и сопоставления Заявок (или протокола преддоговорных переговоров, если проводились) направляет победителю запроса цен проект договора, который составляется путем включения условий исполнения договора, предложенных победителем запроса цен в его Заявке, в проект договора, прилагаемый к Документации с учетом преддоговорных переговоров.

21.2. Договор по результатам запроса цен будет заключен на условиях предложения о цене договора победителя запроса цен: с учетом НДС – с победителем, являющимся налогоплательщиком НДС; без учета НДС – с победителем, применяющим упрощенную систему налогообложения.

21.3. Победитель должен подписать, заверить печатью, направленный ему Заказчиком договор, и представить Заказчику 2 (Два) экземпляра договора в течение 2 (Двух) рабочих дней с момента его получения.

21.4. В случае если победитель запроса цен не представил Заказчику подписанный договор в срок, установленный подпунктом 21.3 настоящей Документации, такой победитель признается уклонившимся от заключения договора.

22. Сведения о возможности Заказчика изменить объем Продукции, предусмотренный договором

22.1. Заказчик по согласованию с Участником, с которым заключен договор по результатам запроса цен, в ходе исполнения договора вправе изменить не более чем на 10 (Десять) процентов предусмотренный договором объем Продукции (товаров, работ, услуг) при изменении потребности Заказчика в Продукции, на приобретение которой заключен договор, или при выявлении потребности в дополнительном объеме Продукции, не предусмотренной договором, но связанных с Продукцией, предусмотренной договором. При этом Заказчик по согласованию с Участником, с которым заключен договор по результатам запроса цен, вправе изменить первоначальную цену договора пропорционально объему такой Продукции, но не более чем на 10 (Десять) процентов такой цены договора.

Приложение №1
к Документации
от «_____» _____ 2020 г.

СПЕЦИФИКАЦИЯ

на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

№ п/ п	Наименование	Кол-во лицензий, шт.
1	Лицензия на программное обеспечение «Falcongaze SecureTower» (контроль: MAIL; WEB; IM; FTP; USB; Printers; Desktop activity; Indexing), Стандартные версии	500
2	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер контроля агентов, Стандартные версии	1
3	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер обработки данных, Стандартные версии	1
4	Лицензия на программное обеспечение "Falcongaze SecureTower», сервер обработки почты, Стандартные версии	1
5	Лицензия на программное обеспечение «Falcongaze SecureTower», перехват сервером обработки почты (контроль e-mails), Стандартные версии	600
6	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания изображений, Стандартные версии	1
7	Лицензия на программное обеспечение «Falcongaze SecureTower», средство распознавания изображений ABBYY, Стандартные версии	500
8	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер расследований инцидентов, Стандартные версии	1
9	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания речи, Стандартные версии	1
10	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер анализа рисков, Стандартные версии	1

Требования к функциональным возможностям программной системы

1. Требования к назначению программной системы

Программная система (далее - Система) должна обеспечивать решение следующих задач:

- мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов вычислительных сетей Заказчика конфиденциальной информации по следующим каналам:
  - электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги);
  - электронная почта, защищенная по стандарту S/MIME;
  - электронная почта, переданная через почтовые веб-службы (Gmail.com, Hotmail.com, Mail.ru, Rambler.ru, Yahoo.com, Yandex.ru и т.д.);
  - двунаправленный перехват сообщений в чатах, статусов, комментариев к публикациям и на форумах социальных сетей: Facebook, Twitter, ВКонтакте, Одноклассники;
  - средства мгновенного обмена сообщениями – SIP, Skype, Telegram, Viber (с возможностью перехвата и архивирования вложенных файлов, текстовых и голосовых данных), Microsoft Lync (голосовые и текстовые сообщения), Slack (текстовые сообщения и файлы), AIM, ICQ, Miranda, Mail.Ru Агент, Google Hangouts, PSI, QIP Infium, WhatsApp, Yahoo! Messenger и др., в т.ч. использующие шифрование;
  - запись файлов на внешние накопители;
  - запись файлов на локальные сетевые ресурсы;
  - отправка файлов в облачные сервисы хранения информации (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск);
  - отправка файлов на печать на локальные и сетевые принтеры;
  - передача файлов в компьютерных сетях по протоколам FTP и FTPS;
- мониторинг событий разглашения конфиденциальной информации в разговорной речи путем контроля аудио потока с микрофона контролируемой рабочей станции в режиме реального времени;
- поддержка удаленного доступа к просмотру видеоизображения рабочего стола компьютера пользователя в режиме реального времени;
- мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов;
- сбор и хранение всех исходящих и входящих электронных сообщений, с возможностью полнотекстового поиска по архиву, в том числе и в присоединенных к письмам файлах;
- поиск информации и формирование политик безопасности по группам Active Directory;
- контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного назначения);
- контроль эффективности использования рабочего времени и ресурсов персоналом компании путем снятия снимков экрана, сбора информации по времени работы/простоя ПК, используемым приложениям (в том числе WinRT (Metro) и виртуальные рабочие столы), а также статистического и событийного анализа перехваченной информации;
- контроль инцидентов безопасности и анализ присвоенных им показателей уровня риска;
- запрет запуска отдельных программных приложений;
- возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности);
- блокирование сетевого трафика отдельных процессов;
- возможность блокирования передачи исходящих сообщений по протоколам SMTP, HTTP и MAPI (в т.ч. с использованием шифрования), содержащих определенную информацию на основе контентного и атрибутивного анализа сообщений и вложенных данных.

2. Требования к техническим и функциональным характеристикам системы

Система должна поддерживать несколько схем перехвата трафика в контролируемой сети, а также их комбинации:

- централизованный перехват данных с сетевого коммутатора;
- перехват данных с рабочих станций пользователей;

- перехват электронной почты, переданной через почтовые сервера;
- перехват HTTP(S)-трафика, переданного через прокси-сервера.

2.1 Требования к реализации централизованного перехвата данных

Система должна обеспечивать:

- перехват данных, отправляемых по протоколам, не использующим шифрование (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M) ;
- фильтрация данных, отправляемых по протоколу HTTP;
- гибкая настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным MAC-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, процессам.

2.2 Требования к перехвату данных с рабочих станций

Система должна поддерживать установку независимых программных модулей контроля непосредственно на рабочие станции сети организации.

Модуль должен осуществлять перехват нешифрованного сетевого трафика, а также выполнять перехват SSL-трафика и данных, переданных по использующим шифрование протоколам.

Модуль должен фиксировать активность пользователя на контролируемой рабочей станции.

Контроль рабочих станций должен обеспечивать следующее:

- возможность как централизованной установки модулей - из единой консоли управления либо средствами групповых политик домена (с использованием MSI-пакета), так и установки вручную (с использованием отдельного EXE-инсталлятора модуля с графическим интерфейсом);
- централизованная настройка дистрибутива модуля для установки вручную;
- возможность перехвата данных, отправляемых по нешифрованным протоколам (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M);
- возможность перехвата данных, отправляемых по шифрованным протоколам (с использованием SSL/TLS-шифрования), включая шифрованные протоколы передачи веб-трафика (HTTPS), корпоративной и внешней электронной почты (IMAPS, POP3S, SMTPS, MAPI over RPC over HTTP, MAPI over RPC, MAPI over HTTPS), мессенджеров, передачи файлов (FTPS), а также данных, переданных в облачных сервисах (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск) и приложениях Google Hangouts, Microsoft Lync, SIP, Skype, Telegram, Viber, WhatsApp;
- перехват данных, отправляемых по протоколам с использованием SSL/TLS-шифрования, осуществляется путем подмены цифрового сертификата. При этом должна поддерживаться возможность указания произвольного имени удостоверяющего центра в генерируемых системой сертификатах, а также возможность гибкой настройки подмены для использования различных сертификатов при перехвате различных SSL/TLS-соединений;
- возможность перехвата и автоматического дешифрования зашифрованных почтовых сообщений, содержащих цифровую подпись (включая вложенные в письма файлы), защищенных по стандарту S/MIME;
- возможность установки режима перехвата: только шифрованный либо нешифрованный трафик, весь трафик (шифрованный и нешифрованный);
- возможность создания политик фильтрации и блокирования трафика на основании атрибутов и содержимого перехватываемых данных;
- возможность фильтрации данных, отправляемых по протоколу HTTP/ HTTPS;
- возможность гибкой настройки исключений из перехвата по IP- адресам (отдельным и диапазону), протоколам, системным учетным записям пользователей, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, атрибутам процессов, вешним устройствам и локальным сетевым ресурсам;
- возможность блокирования передачи исходящих сообщений по протоколу SMTP(S) на основании заданных политик;
- возможность указания адресов электронной почты пользователей, активных в текущий момент, на компьютерах с установленными агентами.
- возможность блокирования передачи почтовых сообщений по протоколу MAPI (в том числе с использованием шифрования), содержащих определенную информацию (на основании заданных

политик безопасности с использованием контентного и атрибутивного анализа сообщений и вложенных данных, на основании имени домена, DNS-имени и SID домена, имени компьютера и пользователя);

- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных);
- возможность блокирования посещения веб-ресурсов;
- блокирование поиска запрещенной информации в сети Интернет;
- возможность блокирования паразитного HTTP(S) трафика вредоносных и служебных программ;
- блокирование сетевого трафика процессов на основании их атрибутов и значения хеш-функций исполнительных файлов;
- настройка уведомлений пользователя рабочей станции о сработках блокировки устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика;
- настройка сообщений о блокировании устройств, запуска процессов, сетевого трафика процессов, HTTP- и MAPI-трафика;
- перехват web-коммуникаций пользователей в социальных сетях Facebook, Twitter, ВКонтакте, Одноклассники. При этом должны поддерживаться: двунаправленный перехват сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев;
- перехват входящей и исходящей web-почты (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex) ;
- контроль данных, отправляемых на внешние накопители, принтеры, облачные хранилища и локальные сетевые ресурсы пользователей и терминальных серверов;
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к локальным сетевым ресурсам;
- аудит файловых операций, контроль передачи информации и блокирование доступа пользователей к облачным сервисам хранения информации при использовании веб-интерфейса и десктоп-приложений (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск);
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к различным классам внешних накопителей информации с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер);
- аудит использования и контроль доступа для внешних устройств, подключенных к рабочей станции, и блокирование доступа с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- возможность сбора статистики по времени работы/простоя компьютера;
- контроль запуска приложений на компьютерах пользователей, а также длительность работы в каждом приложении (например, контроль использования нежелательного или запрещенного программного обеспечения в корпоративной сети);
- запрет запуска отдельных программных приложений на контролируемой рабочей станции на основании имени процесса, атрибутов исполнительного файла и значения хеш-функции;
- возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (нажатие клавиши Print Screen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения, блокировка каких-либо операций);
- перехват данных, помещаемых в буфер обмена с поддержкой исключения активности отдельных процессов из перехвата;
- контроль данных, вводимых пользователем с клавиатуры («кейлоггер») с возможностью исключения активности отдельных процессов из перехвата;
- прослушивание аудиопотока, поступающего с микрофонов, подключенных к рабочим станциям в режиме реального времени;
- возможность удаленного просмотра видеоизображения рабочего стола пользователя в режиме реального времени;
- автоматическая запись аудиопотока с микрофона и системных звуков, а также видеоизображения с рабочего стола и подключенной веб-камеры компьютера по расписанию;
- запись аудио- и видеопотоков вручную;
- автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя (по имени, по заданным атрибутам или значениям хеш-функций);

- настройка функциональных возможностей модулей применительно к различным объектам AD, отдельным компьютерам (группам компьютеров) и пользователям с указанным SID;
- выбор условий активации настроек модулей, например, наличие соединения с сервером, наличие активного VPN-подключения, произвольное заданное условие;
- возможность защиты модуля на рабочей станции от несанкционированного удаления пользователем;
- возможность скрытия модуля на рабочей станции (включая скрытие процессов, служб, установочных файлов и папок);
- опциональное отображение иконки системы в панели задач контролируемой рабочей станции;
- сохранение функциональных возможностей модуля (автономный режим) в случае выноса рабочей станции за пределы корпоративной сети, сохранение всех данных перехвата. Автоматическое восстановление связи с серверной частью системы;
- возможность настройки автономного режима работы модуля;

Система должна отслеживать и отображать статистику по состоянию модулей контроля рабочих станций:

- поступление данных на сервер от каждого модуля,
- пользователей, контролируемых модулем;
- подключенные внешние устройства
- типы перехватываемых данных (протоколов).

Данные статистики должны быть доступны для экспорта.

2.3 Требования к перехвату HTTP-трафика, переданного через прокси-сервера

Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервера должен обеспечивать:

- возможность перехвата и фильтрации данных;
- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S) на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных.

2.4 Требования к перехвату электронной почты, переданной через почтовые сервера

Система должна поддерживать интеграцию с почтовыми серверами, развернутыми на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного обеспечения, обеспечивающего перехват всех почтовых сообщений, переданных и полученных с помощью почтовых серверов по протоколам POP3, SMTP, IMAP и MAPI.

2.5 Требования к функциям хранения и обработки данных

В части хранения и обработки данных система должна обеспечивать:

- хранение всех перехватываемых данных вне зависимости от настроек политик безопасности, настроенных средствами системы;
- возможность централизованного хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL, MySQL (на выбор);
- возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз. Поисковые операции выполняются по всем базам данных в группе. Для событий запуска ротации можно настроить выполнение скриптов (перед и/или после ротации);
- поддержка работы с базами данных, расположенных на разных серверах;
- возможность настройки правил записи данных в базы для регуляции, в какую базу или группу баз записывать информацию в зависимости от типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутной информации;
- возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно;
- возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;

- возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- возможность настройки расписания для репликации данных;
- возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;
- при переполнении очереди репликации сервер блокирует прием новых данных;
- отображение статистики репликации данных;
- возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;
- возможность сохранения файловых объектов большого размера на диск сервера, а не в базу. В базу данных при этом помещаются относительные пути к файлам;
- возможность настройки длительности хранения информации в базе данных в группе ротации, в том числе установки различной длительности хранения для различных типов данных (например, хранить почтовую переписку за последние 60 дней, а переписку через мессенджеры – за последние 30 дней);
- возможность очистки базы данных вручную через Консоль администратора;
- возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);
- возможность архивирования баз данных с последующим подключением к системе для осуществления поиска в них критичной информации;
- параллельную обработку данных, перехваченных по различным каналам передачи информации;
- настройку резервного хранилища модуля контроля рабочих станций в части ограничения размера и максимального периода хранения информации;
- настройку максимальной скорости передачи перехваченных данных с рабочих станций модулем контроля на сервер;
- асинхронный поиск по перехваченным данным (отображение результатов должно выполняться по мере их получения).
- возможность выборочного удаления пользователем перехваченной информации.

2.6 Требования к поддерживаемым форматам файлов

Система должна поддерживать обработку файлов следующих форматов:

- Adobe Acrobat (*.pdf)
- Ami Pro (*.sam)
- Ansi Text (*.txt)
- ASCII Text
- ASF (метаданные) (*.asf)
- CSV (Comma-separated values) (*.csv)
- DBF (*.dbf)
- DjVu
- DWG
- DXF
- EBCDIC
- EML files (электронные письма, сохраненные Outlook Express) (*.eml)
- Enhanced Metafile Format (*.emf)
- Eudora MBX файлы сообщений (*.mbx)
- Flash (*.swf)
- GZIP (*.gz)
- HTML (*.htm, *.html)
- JPEG (метаданные) (*.jpg)
- Lotus 1-2-3 (*.wk?, *.123)
- MBOX архивы электронных писем (включая Thunderbird) (*.mbx)
- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht)
- Microsoft Access (*.mdb)
- Microsoft Access 2007 (*.accdb)
- Microsoft Document Imaging (*.mdi)

- Microsoft Excel (*.xls)
- Microsoft Excel 2003 XML (*.xml)
- Microsoft Excel 2007 (*.xlsx)
- Microsoft Open XML Paper Specification (*.oxps)
- Microsoft Outlook (OST)
- Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx)
- Microsoft PowerPoint (*.ppt)
- Microsoft Rich Text Format (*.rtf)
- Microsoft Searchable Tiff (*.tiff)
- Microsoft Word 2003 XML (*.xml)
- Microsoft Word 2007 (*.docx)
- Microsoft Word for DOS (*.doc)
- Microsoft Word for Windows (*.doc)
- Microsoft Works (*.wks)
- MIME-сообщения
- MP3 (метаданные) (*.mp3)
- MSG files (электронные письма, сохраненные Outlook) (*.msg)
- Multimate Advantage II (*.dox)
- Multimate version 4 (*.doc)
- OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений)
- OST (внутренний формат Microsoft Outlook)
- Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)
- TAR (*.tar)
- TIFF (*.tif)
- TNEF (winmail.dat)
- Treepad HJT (*.hjt)
- Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)
- Windows Metafile Format (*.wmf)
- WMA видео (метаданные) (*.wma)
- WMV видео (метаданные) (*.wmv)
- WordPerfect (5.0 и выше) (*.wpd, *.wpf)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordStar 2000
- WordStar версий 1, 2, 3, 4, 5, 6 (*.ws)
- Write (*.wri)
- XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf)
- XML Paper Specification (*.xps)
- XSL
- XyWrite
- ZIP (*.zip)

Кроме того, система должна обеспечивать распознавание и анализ текстовой информации в файлах графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR). Должна поддерживаться возможность выбора между встроенным и сторонним средствами распознавания.

2.7 Требования к возможностям управления пользователями

В системе должно быть обеспечено следующее:

- создание внутренних профилей (карточек) пользователей, содержащих всю идентификационную информацию пользователей локальной сети;
- интеграция с Active Directory (возможность импорта всех идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя; возможность автоматического создания (удаления) профилей пользователей при добавлении (удалении) записей в (из) Active Directory,

автоматическое создание карточек при обнаружении ранее не известной пользовательской информации, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями с возможностью настройки расписания синхронизации);
- возможность выборочной интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;
- возможность автоматической привязки идентификационных данных пользователя, отсутствующих в Active Directory (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя;
- возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей (например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании);
- возможность создания и редактирования пользовательских карточек;
- возможность отображения пользовательских карточек как в виде линейного списка, так и с разбивкой на группы и подгруппы на основании информации из Active Directory (с учетом Organizational Units), либо на основании задаваемых параметров в карточках пользователей (произвольная группировка по организациям/отделам);
- аутентификация пользователей, работающих с системой, на основании их учетных записей Windows и на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);
- возможность разграничения прав доступа к системе и ее компонентам для различных пользователей с назначением ролей (например, «системный администратор» - доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения» - доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности» - доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) на основе аутентификации пользователей;
- политика сложности и срока действия паролей в режиме внутренней аутентификации;
- возможность отправки администратору уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения и т.д.);
- ведение журнала (лога) действий пользователей, работающих с системой.

3. Требования к перечню контролируемых каналов утечки

3.1 Требования к контролю электронной почты

Система должна обеспечивать контроль отправки информации посредством электронной почты, включая следующие возможности:
- перехват почтовых сообщений для нешифрованных и шифрованных (SSL) протоколов – IMAP, POP3, SMTP, MAPI плюс шифрованные аналоги;
- перехват почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME с автоматической расшифровкой содержимого письма;
- перехват почтовых сообщений путем интеграции с почтовыми серверами (на базе Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail и др.) по протоколам IMAP, POP3, SMTP (на выбор);
- перехват почтовых сообщений между Microsoft Outlook и Microsoft Exchange Server по протоколу MAPI (в том числе с использованием шифрования) путем интеграции с Microsoft Outlook;
- перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
- перехват и анализ файлов-вложений почтовых сообщений;
- автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой

уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- блокировка исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений;
- возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;
- возможность поиска по тексту и атрибутам почтовых сообщений и файлов, переданных по почте.

3.2 Требования к контролю IM-клиентов

Система должна обеспечивать контроль отправки информации посредством IM-клиентов, включая следующие возможности:
- перехват сообщений и файлов посредством зеркалирования трафика на сетевом коммутаторе (для протоколов MRA, OSCAR, XMPP, YMSG, не использующих шифрование);
- возможность перехвата текстовых сообщений модулями, установленными на рабочие станции пользователей (Google Hangouts, Microsoft Lync, MRA, OSCAR, SIP, Skype, Slack, Telegram, Viber, WhatsApp, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);
- возможность перехвата файлов, отправляемых с рабочих станций (Microsoft Lync, MRA, OSCAR, Skype, Slack, Telegram, Viber, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);
- возможность перехвата голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber и по протоколу SIP с сохранением разговоров;
- возможность распознавания (перевода в текстовый формат) голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber и SIP;
- возможность воспроизведения сохраненных разговоров Telegram, Skype, Viber, Microsoft Lync и SIP;
- возможность ограничения перехвата по отдельным учетным записям пользователей;
- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через IM-клиенты.

3.3 Требования к контролю HTTP-протокола

Система должна обеспечивать контроль отправки информации по HTTP-протоколу, включая:
- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола HTTP);
- возможность перехвата посредством интеграции с прокси-серверами по протоколу ICAP (для протоколов HTTP и HTTPS);
- возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов HTTP и HTTPS);
- возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;
- возможность создания и гибкой настройки фильтров для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователем;
- возможность настройки фильтрации перехвата данных по MIME-типам;
- перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;
- перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
- перехват сообщений, переданных в веб-клиентах ICQ и Skype ;
- перехват и анализ поисковых запросов пользователя;
- сохранение адресов всех страниц (URL), посещенных пользователем;

- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);
- возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов определенного содержания (HTTP и HTTPS);
- контроль браузер-активности (посещения веб-сайтов с помощью веб-браузера): фиксация переходов между страницами веб-сайтов и ведение комплексной статистики времени, проведенного на различных веб-ресурсах.

3.4 Требования к контролю FTP-протокола

Система должна обеспечивать контроль информации, передаваемой по протоколу FTP, включая возможности:

- перехвата файлов, загруженных или переданных по простому FTP-соединению, а также переданных по зашифрованному SSL-соединению;
- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола FTP);
- возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов FTP и FTPS);
- возможность настройки ограничения по размеру перехватываемых файлов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S).

3.5 Требования к контролю принтеров

Система должна обеспечивать контроль информации, отправляемой на печать, включая:

- возможность перехвата документов, отправляемых на сетевые и локальные принтеры (в том числе подключенные к COM-, LPT-портам);
- возможность перехвата печати в XPS-формат;
- возможность настройки исключений из перехвата по отдельным принтерам;
- возможность ограничения перехвата печати по количеству страниц и по размеру документа;
- возможность исключения процессов для модуля перехвата печати на принтерах.
- извлечение и анализ текста отправленных на печать документов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам отправленных на печать файлов;
- сохранение перехваченного текста (PDF и HTML-формат).

3.6 Требования к контролю подключенных устройств и внешних накопителей информации

Система должна обеспечивать контроль информации, отправляемой на внешние носители, включая:

- теневое копирование файлов, отправляемых на внешние накопители информации (съемные жесткие диски, карты памяти, съемные накопители, CD/DVD и флоппи-диски);
- возможность настройки исключений из теневого копирования по размеру и расширению файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- возможность настройки исключений из теневого копирования для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);

- контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- управление правами записи на внешние накопители информации с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;
- возможность контроля копирования информации на внешние накопители информации как в локальных, так и терминальных пользовательских сессиях;
- аудит событий копирования файлов на внешние накопители: должно фиксироваться имя файла, пользователь, дата, время и данные устройства;
- контроль доступа и аудит использования внешних устройств любого типа, подключаемых к рабочей станции, по набору параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам файлов, отправленных на внешние накопители информации.

3.7 Требования к контролю локальных сетевых ресурсов

Система должна обеспечивать контроль информации, отправляемой на локальные сетевые ресурсы, включая следующие возможности:

- теневое копирование файлов, отправляемых на сетевые ресурсы;
- возможность настройки исключений из теневого копирования по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- контроль доступа к сетевым ресурсам с возможностью запрета доступа для определенных пользователей;
- управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;
- возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;
- автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий копирования файлов на локальные сетевые ресурсы: фиксация имени файла, пользователь, дата, время и сетевой путь к ресурсу;
- возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов.

3.8 Требования к контролю облачных хранилищ (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск)

Система должна обеспечивать контроль использования облачных хранилищ, в том числе:

- теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;
- возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

- контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;
- управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;
- автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий отправки файлов в облачные хранилища с фиксацией имени файла, имени пользователя, даты, времени и имени облачного сервиса хранения;
- возможность поиска по тексту и атрибутам отправленных файлов.

4. Требования к возможностям мониторинга действий пользователей на ПК

4.1 Требования к функции снятия скриншотов

Система должна выполнять сохранение снимков рабочего стола пользователей и обеспечивать:

- возможность снятия скриншотов с заданным интервалом с точностью до секунды;
- возможность снятия скриншотов при смене активного окна и смене вкладки браузера, запуске нового процесса;
- возможность снятия скриншотов при срабатывании правила блокировки;
- возможность снятия скриншотов при нажатии клавиши Print Screen;
- возможность настройки качества скриншотов (в т.ч. сохранения в черно-белом формате);
- возможность настройки размера скриншотов (в процентах от оригинала);
- возможность настройки формата скриншотов (JPEG, PNG);
- сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);
- возможность отключения захвата снимков при простое рабочей станции;
- возможность экспорта снимков экранов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;
- возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
- возможность сохранения скриншотов нескольких пользователей за выбранный интервал дат в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
- при просмотре скриншота отображается «watermark» с названием компьютера и именем пользователя.

4.2 Требования к функции сбора статистики по активности ПК

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции:

- ведение статистики по времени работы и простоя (отсутствия действий пользователя) ПК с представлением собранной информации в виде графика;
- ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
- возможность настройки исключений отдельных процессов из мониторинга;
- возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в виде PDF-файла;
- возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу.

4.3 Требования к контролю буфера обмена

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции:

- теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
- возможность ограничения максимального объема текста, перехватываемого из буфера обмена;
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, помещаемому пользователями в буфер обмена.

4.4 Требования к функциям кейлоггера

Система должна поддерживать:

- регистрацию нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных клавиш (Shift, Enter, Backspace и т.п.);
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, вводимому пользователями с клавиатуры.

4.5 Аудиомониторинг

Система должна обеспечивать возможность прослушивания звуковых потоков с рабочей станции, в том числе:

- подключение к микрофонам контролируемых рабочих станций с возможность прослушивания аудиопотока в режиме реального времени;
- прослушивание микрофонов нескольких пользователей одновременно;
- автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;
- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.6 Видеомониторинг

Система должна поддерживать:

- подключение к монитору компьютера пользователя и просмотра изображения рабочего стола в режиме реального времени;
- мониторинг рабочих столов нескольких пользователей одновременно;
- возможность вывода окна просмотра на отдельный экран;
- автоматическая запись видеоизображения рабочего стола и подключенной веб-камеры по расписанию;
- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.7 Требования к контролю файловых систем:

Контроль файловых систем должен позволять:

- формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;
- автоматическое сканирование дисков контролируемых компьютеров на предмет наличия определенных документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;
- возможность выбора компьютеров и пользователей, чьи файловые системы будут контролироваться;
- гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;
- возможность создавать индивидуальные политики контроля за содержимым файловых систем для

отдельных пользователей и рабочих станций;
- возможность удаленного поиска документов в файловых системах контролируемых рабочих станций на основе атрибутов файлов и значения их хеш-функций.

5. Требования к методам анализа перехваченной информации и процедурам реагирования на инциденты безопасности

Система должна обеспечивать следующие функциональные возможности при работе с политиками безопасности:

- автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента); уведомление содержит общую информацию об инциденте (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента), а также ссылку на открытие соответствующего инцидента в пользовательской консоли;
- возможность указания групп Active Directory, к которым могут быть применены политики безопасности;
- возможность добавлять/исключать/редактировать категории и уровни риска инцидентов сервера безопасности для автоматического расчёта показателей уровней риска пользователей;
- возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.);
- возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли (с индивидуальным выделением просмотренных/непросмотренных инцидентов для каждого офицера безопасности, работающего с системой);
- при просмотре информации об инциденте в клиентской консоли доступна следующая информация:
  - пользователь, допустивший нарушение;
  - дата и время инцидента;
  - показатель присвоенного уровня риска;
  - тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.);
  - содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности;
  - другая дополнительная информация.
- возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);
- возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые (непросмотренные) инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);
- возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);
- возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);
- возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;
- возможность экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);
- возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;
- ведение журнала (лога) действий офицера безопасности.

При анализе информации должны быть реализованы следующие возможности (аналитические возможности системы должны быть одинаковы для всех поддерживаемых языков анализируемой информации – включая анализ информации на английском, арабском, белорусском, испанском, казахском, китайском, корейском, немецком, русском и других языках):

Контентный анализ:

- поиск по словам и словосочетаниям с учетом морфологии (возможность отключения), расстояния между словами и порядка слов, транслитерации кириллических символов латинскими, а также с возможностью нечеткого поиска (для поиска ключевых слов, в т.ч. написанных с ошибками и опечатками);
- поддержка регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;
- поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок/регулярных выражений в словарях, с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре);
- поиск документов с умышленно измененным расширением;
- поиск документов, защищенных паролем;
- цифровые отпечатки документов: возможность создания цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента совпадения);
- цифровые отпечатки баз данных: возможность настройки подключения системы к базе данных, содержащей конфиденциальную информацию, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой БД (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»). Создание и обновление цифровых отпечатков баз данных должно осуществляться без промежуточных действий (таких как выгрузка базы данных в файл-источник цифрового отпечатка). При внесении изменений в базу данных система должна автоматически обновлять соответствующие цифровые отпечатки.
- комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ».
- поиск данных по DNS-имени и SID компьютера, по имени и SID домена среди данных, перехваченных агентами.
- поиск информации по группам Active Directory.

Анализ по атрибутам

- анализ по атрибутам пользовательских документов, таким как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «размер» и пр.;
- анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных.
- анализ атрибутов процессов: имя исполняющего файла, полный путь к файлу, заголовок окна процесса.

Статистический анализ

- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем электронным письмам (например, «пользователь получил более 10 писем за час» или «пользователь отправил менее 20 писем за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем файлам (например, «пользователь получил более 10 файлов за час» или «пользователь отправил более 20 файлов за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по переписке пользователя в IM-клиентах (например, «пользователь провел более 10 сессий переписки за день» или «пользователь отправил более 100 сообщений за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по голосовым переговорам в IM-клиентах (например, «время голосовых переговоров

пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);

- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по посещенным пользователем URL (например, «пользователь посетил более 100 URL за день», «пользователь посетил более 1000 URL за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по поисковым запросам пользователя (например, «пользователь отправил более 100 поисковых запросов в период с 13:00 до 15:00» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по данным, отправленным пользователем на печать (например, «пользователь распечатал более 10 документов за день» или «пользователь распечатал более 1000 страниц за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности/простоя ПК (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени работы пользователя с определенными приложениями (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

Событийный анализ

Возможность настройки автоматических уведомлений в следующих случаях:

- выявления факта запуска (завершения) пользователем определенного приложения;
- обнаружения пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);
- копирования файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;
- подключения и использования на контролируемых рабочих станциях устройств с определенными параметрами;
- блокирования пересылки данных по SMTP, HTTP, MAPI;
- посещение определенных web-ресурсов;
- обнаружения конфиденциальных файлов на компьютерных дисках пользователей;
- выявления факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения).

Анализ рисков

Возможность дополнить политики безопасности следующим функционалом:

- формировать модели поведения сотрудников и задавать им соответствующий уровень риска;
- информировать специалистов отдела безопасности об уровне риска и об инцидентах политик безопасности, которые вызвали изменения уровней риска;
- отслеживать изменения в поведении сотрудников в режиме реального времени.

Независимо от используемого типа анализа, система должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных данных (для выявления фактов нарушения вновь созданной политики безопасности в прошлом за весь период наблюдения).

6. Организация документов при проведении расследований

Система должна предусматривать специальный модуль для организации информации и документации для проведения расследований (типа «центр расследований»), который должен обеспечивать следующие возможности:

- в целях сбора доказательств по инцидентам безопасности -- создание документа (дела), который может включать в себя:

- информацию об инциденте;
- перечень вовлеченных лиц и их реквизиты;
- перечень проводимых (проведенных) мероприятий по расследованию инцидента и их результаты;
- выводы по результатам расследований;
- материалы расследований – внутренние документы (результаты перехвата) системы;
- реквизиты внутренних документов: тип данных, локальный пользователь, удаленный пользователь, дата перехвата, размер документа;
- материалы расследований – внешние документы;
- внешние документы, содержащие аналитические записки, рапорты и т.п.

- в целях комплексного аудита результатов перехвата обеспечивать функции:
- просмотр содержания документов в расширенном виде напрямую из дела;
- фильтрацию документов при просмотре в деле;
- представление включенных в дело документов в режимах просмотра карточки, список;
- возможность экспорта дела в форматы *.pdf, *.xps.
- возможность распечатки дела на принтере.

- в целях контроля за внесением изменений в дело наличие журнала событий, включающего в себя информацию о всех вносимых правках:
- имя пользователя, который совершил операцию в деле;
- совершенное действие;
- дату и время совершенного действия;
- прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.

- в целях упрощения работы лиц, ведущих расследование обеспечивать:
- ведение списка дел;
- возможность сортировки дел в группы;
- возможность создания групп и подгрупп с количество уровней иерархии не менее 20;
- возможность переноса дел из группы в группу простым перетаскиванием «мышкой»;
- возможность переноса подгрупп из группы в группу простым перетаскиванием «мышкой»;
- возможность удаления дел и групп;
- возможность исправления дел;
- возможность просмотра: всех дел, только открытых дел, только закрытых дел;
- возможность глубокой пользовательской настройки просмотра дел: всех дел за определенный период; дел, открытых в определенный период; дел, закрытых в определенный период;
- возможность закрепления и открепления поля списка дел;
- возможность переноса поля списка дел к любой стороне окна программы.

Система также должна обеспечивать возможность удобного присоединения документов к делу в модуле типа «центр расследований» из других модулей системы: например, через контекстное меню.

7. Требования к отчетности

Все перехваченные данные должны представляться в форме отчетов следующих видов:

Отчет об активности пользователя

- Вкладка «Дневная активность» на временной сетке с шагом в 1 час должна содержать:
- информацию о количестве отправленных и полученных пользователем писем;
- информацию о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;
- информацию о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах;
- информацию о количестве посещенных URL и отправленных поисковых запросов;
- информацию о количестве сделанных системой снимков экрана рабочего стола пользователя;
- информацию о времени работы/простоя компьютера пользователя, детальную статистику активности приложений и данные о процентном соотношении времени работы в различных приложениях;

- информацию о количестве документов, помещенных в буфер обмена;
- информацию о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;
- информацию о количестве символов, введенных пользователем с клавиатуры.

Вкладка должна быть интерактивная и динамическая, чтобы позволять осуществлять переход по ссылкам непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок.

Должна быть обеспечена возможность экспорта дневной активности во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к перехваченным данным в веб-браузере, а также с возможностью сохранения выбора ассоциированных просмотрищиков для разных типов документов в расширенных настройках.

- Вкладка «Статистика по активности»

Система должна представлять данные, собранные по определенному пользователю за конкретный интервал времени, в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов).

Графики по типам информации должны поддерживать интерактивность и динамичность, поддерживать возможность перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов.

Необходимо предусмотреть возможность сохранения статистики во внешний файл формата PDF и XPS.

- Вкладка «Взаимосвязи»

Система должна обладать возможностью графического отображения взаимосвязей пользователя (в виде графа или таблицы) на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь обменивался какой-либо информацией в течение выбранного интервала времени.

Должна быть обеспечена поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.

Возможность просмотра взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.

Возможность выбора масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).

Возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.

Поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

Отчет по пользователям

Система должна реализовывать возможность построения сводного интерактивного отчета по определенному пользователю за все время наблюдения (или за выбранный интервал времени), включающего следующую информацию:

- статистика перехвата данных, в том числе
  - количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;
  - количество посещенных сайтов и поисковых запросов;
  - количество файлов, переданных/принятых по FTP;
  - количество распечатанных документов и страниц;
  - количество операций копирования в буфер обмена;
  - количество снятых скриншотов;
  - количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;
  - количество нажатых клавиш клавиатуры.
- информация об активности пользователя за компьютером, в том числе
  - общее время активной работы пользователя за ПК;
  - среднесуточное время активной работы пользователя за ПК;
  - общее время простоя ПК;
  - среднесуточное время простоя ПК;

- общее время присутствия сотрудника на работе;
- среднесуточное время присутствия сотрудника на работе;
- среднее время начала работы;
- среднее время окончания работы;
- общее количество рабочих дней;
- календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой);
- гистограмма по времени активности/простоя компьютера пользователя за каждый день.

- информация об активности приложений на компьютере пользователя, в том числе
  - процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы);
  - полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них.
- информация о браузер-активности, в том числе
  - рейтинг посещенных веб-ресурсов;
  - хронология активности в веб-браузере.
- информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.

  Необходимо предусмотреть возможность пакетного сохранения отчетов для групп пользователей с предварительной настройкой единой формы отчета.

  ТОП-отчет по пользователям

  Система должна обеспечивать создание сводных интерактивных отчетов по всем контролируемым каналам передачи данных за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, наиболее активно использующих этот канал.

  Система должна содержать возможность построения ТОП-отчета для сотрудников, входящих в группы пользователей системы либо в группы пользователей Active Directory.

  Необходимо предусмотреть возможность построения сводных отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз.

  При создании отчетов должна быть обеспечена возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов, то есть «Браузер активность: количество посещенных сайтов» и «Браузер активность: время проведенное на сайте».

  тчет по политикам безопасности

  Система должна обеспечивать возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, заданных в модуле Политики безопасности.

  При этом система должна обеспечивать просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр итогового количества срабатываний по каждому правилу в отдельности и по всем существующим правилам безопасности.

  Сводный отчет по пользователям

  Система должна предусматривать возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей.

  Также необходимо обеспечить просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики для выбранных статистических показателей.

8. Мониторинг работоспособности системы

Система должна поддерживать:

- ведение журнала событий серверных компонентов системы;

- просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;
- фильтрацию событий в журнале по рабочей станции, серверному компоненту, уровню, дате;
- выбор определенных рабочих станций для ведения мониторинга;
- автоматическое уведомление администратора системы о новых событиях серверных компонентов через консоль администратора и по почте;
- настройку правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

Систем должна фиксировать сведения о всех наиболее существенных событиях в работе серверных компонентов в журнале операционной системы рабочей станции, на которой они установлены.

9. Прочие требования

В процессе своего функционирования система не должна оказывать негативного влияния на функционирование прикладных ИС Заказчика.

Масштабируемость системы

В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы:

- возможность установки нескольких серверов перехвата данных для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;
- возможность установки нескольких серверов контроля агентов для контроля разных сегментов сети или разных групп компьютеров;
- возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;
- возможность установки нескольких серверов индексирования для оптимизации и распределения нагрузки на сервер и базу данных;
- возможность установки нескольких серверов обработки почты для работы с несколькими почтовыми серверами (MS Exchange, IBM Lotus Domino и др.).

Ориентация работы всех компонентов системы на многопоточность

Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах. С помощью добавочного модуля распознавания ABBYY должна существовать возможность распознавания одновременно нескольких PDF-документов.

Удобство администрирования

Система должна обеспечивать следующие функции, повышающие эффективность администрирования программы:

- Централизованное управление компонентами системы с использованием шифрования из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ).
- Возможность централизованного подключения и настройки хранилищ информации, а также создания резервной копии конфигурации всех серверных компонентов с поддержкой последующего восстановления настроек серверов через консоль администратора.
- Возможность автоматического переподключения к серверу при разрыве соединения с консолью пользователя.
- Возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности;
- Возможность отключения автоматического управления системным брандмауэром.
- Возможность при настройке профилей для агентов добавлять компьютер в профиль из схемы агентов, а также копировать/перемещать объекты между профилями.
- Автоматическая фиксация пользователей, которые проводят авторизацию или отклонении сервера-компонента на центральном сервере.

Политика лицензирования ПО

Система должна лицензироваться в соответствии с количеством контролируемых пользователей (500 лицензий для рабочих мест, включая 500 лицензий модуля распознавания изображений ABBYY, 600 лицензий на перехват сервером обработки корпоративной почты). При этом недопустимо использование жесткой привязки лицензии к конкретным рабочим станциям или пользователям. Количество приобретенных лицензий должно определять только количество одновременно

контролируемых пользователей, при этом сам список контролируемых может быстро и гибко изменяться в случае необходимости (например, при наличии 100 пользователей в сети и только 50 лицензий – возможность контролировать выборочно сначала одних пользователей, затем других; при этом переназначение лицензионных слотов должно быть возможно не реже 1 раза в сутки).

Система должна предусматривать возможность покомпонентной поставки, т.е. выбора типов контролируемых данных и отключения неиспользуемого функционала на уровне лицензии. Кроме того, лицензии должны быть бессрочны, в состав системы лицензирования должен быть включен 1 год техподдержки, а также внедрение и настройка Системы.

Приложение №2
к Документации

НА БЛАНКЕ ОРГАНИЗАЦИИ

№ _____
«___» _____ 2020 г Кому _____

ЗАЯВКА

на _____,

(указать наименование предмета запроса цен)

_____

(указать наименование и номер Лота, по которому Участник участвует в запросе цен, (в случае, если запрос цен проводится по нескольким лотам)

1. Изучив Документацию о проведении запрос цен на _____ *(указать наименование предмета запроса цен)* _____ *(фирменное наименование (наименование) Участника с указанием организационно-правовой формы, место нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные, сведения о месте жительства (для физического лица), номер контактного телефона)* в лице, _____ *(наименование должности руководителя и его Ф.И.О. (для юридического лица)* направляет настоящую Заявку на участие в запросе цен и сообщает о согласии участвовать в запросе цен на условиях, установленных в Извещении о проведении запроса цен и Документации о проведении запроса цен, и предлагает заключить договор на сумму _____ (сумма прописью) рублей 00 копеек, НДС не облагается на основании п.п. 26 п. 2 ст. 149 Части 2 Налогового кодекса Российской Федерации.

Цена Договора включает в себя все обязательные платежи и расходы, связанные с исполнением договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

2. Мы заявляем, что на момент подачи Заявки на участие в запросе цен «___»_____20_ г. _____ *(указывается наименование и реквизиты запроса цен)*:

- в отношении_____ *(указывается фирменное наименование Участника)* ликвидация не проводится, решение арбитражного суда о признании _____ *(указывается фирменное наименование Участника)* банкротом и об открытии конкурсного производства отсутствует;
- деятельность _____ *(указывается фирменное наименование Участника)* не приостановлена в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях;
- у _____ *(указывается фирменное наименование Участника)* отсутствует задолженность по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год, размер которой превышает двадцать пять процентов балансовой стоимости активов _____ *(указывается фирменное наименование Участника)* по данным бухгалтерской отчетности за последний завершенный отчетный период.
- _____ *(указывается фирменное наименование Участника)* в течение двух лет до момента подачи Заявки на участие в закупке не было(а) привлечено(а) к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях.

3. Мы согласны придерживаться положений настоящей Заявки на участие в запросе цен до момента заключения договора, но в любом случае не менее 45 дней со дня вскрытия конвертов с Заявками на участие в запросе цен. Эта Заявка на участие в запросе цен будет оставаться для нас обязательной и может быть принята в любой момент до наступления вышеуказанных обстоятельств.

4. В случае, если наши предложения будут признаны лучшими, мы берем на себя обязательства подписать договор с автономной некоммерческой организацией «Аналитический центр при Правительстве Российской Федерации» на _____ *(указать наименование предмета запроса цен (лота)* в соответствии с требованиями Документации о проведении запроса цен и условиями наших предложений, в срок, установленный в Документации о проведении запроса цен.

5. В случае принятия решения о заключении с нами договора, мы обязуемся подписать договор на

_____ *(указать наименование предмета запроса цен (лота)* в соответствии с требованиями Документации о проведении запроса цен и условиями наших предложений по цене, содержащихся в настоящей Заявке на участие в запросе цен и установленных в Документации о проведении запроса цен в качестве критериев оценки Заявок на участие в запросе цен.

6. Мы извещены о включении сведений о _____ *(наименование организации или Ф.И.О. Участника)* в Реестр недобросовестных поставщиков Аналитического центра при Правительстве Российской Федерации в случае нашего уклонения от заключения договора.

7. Сообщаем, что для оперативного уведомления нас по вопросам организационного характера и взаимодействия с Заказчиком нами уполномочен _____ *(должность, Ф.И.О., телефон, электронная почта сотрудника – Участника).*

Все сведения о проведении запроса цен просим сообщать уполномоченному лицу.

8. В случае присуждения нам права заключить договор в период с даты получения проекта договора и до подписания официального договора настоящая Заявка на участие в запросе цен будет носить характер предварительного заключенного нами и Заказчиком договора о заключении договора на условиях наших предложений.

9. Наше местонахождение _____ *(для юридического лица)*, место жительства _____ (*для физического лица)*, почтовый адрес _____, телефон _____, факс _____.

10. Корреспонденцию в наш адрес просим направлять по адресу: _____.

11. К настоящей Заявке прилагаются документы на _____стр.

11.1 Приложение № 1

Предложение о функциональных характеристиках (потребительских свойствах) и качественных характеристиках.

11.2. **Копия, действующего на момент подачи заявки, договора, подтверждающего наличие соответствующих полномочий Участника от правообладателя прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower».**

11.3 Приложение № 2

Анкета Участника.

_____ _____

(подпись) (фамилия, имя, отчество подписавшего, должность)

М.П.

Приложение № 1
к Заявке

НА БЛАНКЕ ОРГАНИЗАЦИИ

№ _____
«___» _____ 2020 г. Кому _____

Предложение о функциональных характеристиках (потребительских свойствах) и качественных характеристиках товаров

_____,
(Участник)

наименование (юридического лица)/Ф.И.О. (для физического лица)

согласно на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

Наименование, количество, характеристики и цена приведены в таблице:

№ п/п	Наименование	Кол-во лицензий, шт.	Цена за ед. руб., (без НДС)	Сумма в руб. (без НДС)
1	Лицензия на программное обеспечение «Falcongaze SecureTower» (контроль: MAIL; WEB; IM; FTP; USB; Printers; Desktop activity; Indexing), Стандартные версии	500	*	*
2	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер контроля агентов, Стандартные версии	1	*	*
3	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер обработки данных, Стандартные версии	1	*	*
4	Лицензия на программное обеспечение "Falcongaze SecureTower», сервер обработки почты, Стандартные версии	1	*	*
5	Лицензия на программное обеспечение «Falcongaze SecureTower», перехват сервером обработки почты (контроль e-mails), Стандартные версии	600	*	*
6	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания изображений, Стандартные версии	1	*	*
7	Лицензия на программное обеспечение «Falcongaze SecureTower», средство распознавания изображений ABBYY, Стандартные версии	500	*	*
8	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер расследований инцидентов, Стандартные версии	1	*	*
9	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания речи,	1	*	*

	Стандартные версии			
10	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер анализа рисков, Стандартные версии	1	*	*
Итого				*****

Всего неисключительные права на использование Продукта на сумму _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

** Заполняется Участником запроса цен.*
Текст, выделенный курсивом, в заявке не воспроизводится

Требования к функциональным возможностям программной системы

1. Требования к назначению программной системы

Программная система (далее - Система) должна обеспечивать решение следующих задач:

– мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов вычислительных сетей Заказчика конфиденциальной информации по следующим каналам:

- электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги);
- электронная почта, защищенная по стандарту S/MIME;
- электронная почта, переданная через почтовые веб-службы (Gmail.com, Hotmail.com, Mail.ru, Rambler.ru, Yahoo.com, Yandex.ru и т.д.);
- двунаправленный перехват сообщений в чатах, статусов, комментариев к публикациям и на форумах социальных сетей: Facebook, Twitter, ВКонтакте, Одноклассники;
- средства мгновенного обмена сообщениями – SIP, Skype, Telegram, Viber (с возможностью перехвата и архивирования вложенных файлов, текстовых и голосовых данных), Microsoft Lync (голосовые и текстовые сообщения), Slack (текстовые сообщения и файлы), AIM, ICQ, Miranda, Mail.Ru Агент, Google Hangouts, PSI, QIP Infium, WhatsApp, Yahoo! Messenger и др., в т.ч. использующие шифрование;
- запись файлов на внешние накопители;
- запись файлов на локальные сетевые ресурсы;
- отправка файлов в облачные сервисы хранения информации (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск);
- отправка файлов на печать на локальные и сетевые принтеры;
- передача файлов в компьютерных сетях по протоколам FTP и FTPS;

– мониторинг событий разглашения конфиденциальной информации в разговорной речи путем контроля аудио потока с микрофона контролируемой рабочей станции в режиме реального времени;

– поддержка удаленного доступа к просмотру видеоизображения рабочего стола компьютера пользователя в режиме реального времени;

– мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов;

– сбор и хранение всех исходящих и входящих электронных сообщений, с возможностью полнотекстового поиска по архиву, в том числе и в присоединенных к письмам файлах;

– поиск информации и формирование политик безопасности по группам Active Directory;

– контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного назначения);

– контроль эффективности использования рабочего времени и ресурсов персоналом компании путем снятия снимков экрана, сбора информации по времени работы/простоя ПК, используемым приложениям (в том числе WinRT (Metro) и виртуальные рабочие столы), а также статистического и событийного анализа перехваченной информации;

– контроль инцидентов безопасности и анализ присвоенных им показателей уровня риска;

– запрет запуска отдельных программных приложений;

– возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности);

– блокирование сетевого трафика отдельных процессов;

– возможность блокирования передачи исходящих сообщений по протоколам SMTP, HTTP и MAPI (в т.ч. с использованием шифрования), содержащих определенную информацию на основе контентного и атрибутивного анализа сообщений и вложенных данных.

2. Требования к техническим и функциональным характеристикам системы

Система должна поддерживать несколько схем перехвата трафика в контролируемой сети, а также их комбинации:

– централизованный перехват данных с сетевого коммутатора;

– перехват данных с рабочих станций пользователей;

– перехват электронной почты, переданной через почтовые сервера;

– перехват HTTP(S)-трафика, переданного через прокси-сервера.

2.1 Требования к реализации централизованного перехвата данных

Система должна обеспечивать:

– перехват данных, отправляемых по протоколам, не использующим шифрование (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M) ;

– фильтрация данных, отправляемых по протоколу HTTP;

– гибкая настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным MAC-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, процессам.

2.2 Требования к перехвату данных с рабочих станций

Система должна поддерживать установку независимых программных модулей контроля непосредственно на рабочие станции сети организации.

Модуль должен осуществлять перехват нешифрованного сетевого трафика, а также выполнять перехват SSL-трафика и данных, переданных по использующим шифрование протоколам.

Модуль должен фиксировать активность пользователя на контролируемой рабочей станции.

Контроль рабочих станций должен обеспечивать следующее:

– возможность как централизованной установки модулей - из единой консоли управления либо средствами групповых политик домена (с использованием MSI-пакета), так и установки вручную (с использованием отдельного EXE-инсталлятора модуля с графическим интерфейсом);

– централизованная настройка дистрибутива модуля для установки вручную;

– возможность перехвата данных, отправляемых по нешифрованным протоколам (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M);

– возможность перехвата данных, отправляемых по шифрованным протоколам (с использованием SSL/TLS-шифрования), включая шифрованные протоколы передачи веб-трафика (HTTPS), корпоративной и внешней электронной почты (IMAPS, POP3S, SMTPS, MAPI over RPC over HTTP, MAPI over RPC, MAPI over HTTPS), мессенджеров, передачи файлов (FTPS), а также данных, переданных в облачных сервисах (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск) и приложениях Google Hangouts, Microsoft Lync, SIP, Skype, Telegram, Viber, WhatsApp;

– перехват данных, отправляемых по протоколам с использованием SSL/TLS-шифрования, осуществляется путем подмены цифрового сертификата. При этом должна поддерживаться возможность указания произвольного имени удостоверяющего центра в генерируемых системой сертификатах, а также возможность гибкой настройки подмены для использования различных сертификатов при перехвате различных SSL/TLS-соединений;

– возможность перехвата и автоматического дешифрования зашифрованных почтовых сообщений, содержащих цифровую подпись (включая вложенные в письма файлы), защищенных по стандарту S/MIME;

– возможность установки режима перехвата: только шифрованный либо нешифрованный трафик, весь трафик (шифрованный и нешифрованный);

– возможность создания политик фильтрации и блокирования трафика на основании атрибутов и содержимого перехватываемых данных;

– возможность фильтрации данных, отправляемых по протоколу HTTP/ HTTPS;

– возможность гибкой настройки исключений из перехвата по IP- адресам (отдельным и диапазону), протоколам, системным учетным записям пользователей, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, атрибутам процессов, вешним устройствам и локальным сетевым ресурсам;

– возможность блокирования передачи исходящих сообщений по протоколу SMTP(S) на основании заданных политик;

– возможность указания адресов электронной почты пользователей, активных в текущий момент, на компьютерах с установленными агентами.

– возможность блокирования передачи почтовых сообщений по протоколу MAPI (в том числе с использованием шифрования), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений и вложенных данных, на основании имени домена, DNS-имени и SID домена, имени компьютера и пользователя);

– возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных);

– возможность блокирования посещения веб-ресурсов;

– блокирование поиска запрещенной информации в сети Интернет;

– возможность блокирования паразитного HTTP(S) трафика вредоносных и служебных программ;

– блокирование сетевого трафика процессов на основании их атрибутов и значения хеш-функций исполнительных файлов;

– настройка уведомлений пользователя рабочей станции о сработках блокировки устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика;

– настройка сообщений о блокировании устройств, запуска процессов, сетевого трафика процессов, HTTP- и MAPI-трафика;

– перехват web-коммуникаций пользователей в социальных сетях Facebook, Twitter, ВКонтакте, Одноклассники. При этом должны поддерживаться: двунаправленный перехват сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев;

– перехват входящей и исходящей web-почты (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex) ;

– контроль данных, отправляемых на внешние накопители, принтеры, облачные хранилища и локальные сетевые ресурсы пользователей и терминальных серверов;

– аудит файловых операций, контроль записи информации и блокирование доступа пользователей к локальным сетевым ресурсам;

– аудит файловых операций, контроль передачи информации и блокирование доступа пользователей к облачным сервисам хранения информации при использовании веб-интерфейса и десктоп-приложений (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск);

– аудит файловых операций, контроль записи информации и блокирование доступа пользователей к различным классам внешних накопителей информации с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер);

– аудит использования и контроль доступа для внешних устройств, подключенных к рабочей станции, и блокирование доступа с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);

– возможность сбора статистики по времени работы/простоя компьютера;

– контроль запуска приложений на компьютерах пользователей, а также длительность работы в каждом приложении (например, контроль использования нежелательного или запрещенного программного обеспечения в корпоративной сети);

– запрет запуска отдельных программных приложений на контролируемой рабочей станции на основании имени процесса, атрибутов исполнительного файла и значения хеш-функции;

– возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (нажатие клавиши Print Screen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения, блокировка каких-либо операций);

– перехват данных, помещаемых в буфер обмена с поддержкой исключения активности отдельных процессов из перехвата;

– контроль данных, вводимых пользователем с клавиатуры («кейлоггер») с возможностью исключения активности отдельных процессов из перехвата;

– прослушивание аудиопотока, поступающего с микрофонов, подключенных к рабочим станциям в режиме реального времени;

– возможность удаленного просмотра видеоизображения рабочего стола пользователя в режиме реального времени;

– автоматическая запись аудиопотока с микрофона и системных звуков, а также видеоизображения с рабочего стола и подключенной веб-камеры компьютера по расписанию;

– запись аудио- и видеопотоков вручную;

– автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя (по имени, по заданным атрибутам или значениям хеш-функций);

– настройка функциональных возможностей модулей применительно к различным объектам AD, отдельным компьютерам (группам компьютеров) и пользователям с указанным SID;

– выбор условий активации настроек модулей, например, наличие соединения с сервером, наличие активного VPN-подключения, произвольное заданное условие;

– возможность защиты модуля на рабочей станции от несанкционированного удаления пользователем;

– возможность скрытия модуля на рабочей станции (включая скрытие процессов, служб, установочных файлов и папок);

– опциональное отображение иконки системы в панели задач контролируемой рабочей станции;

– сохранение функциональных возможностей модуля (автономный режим) в случае выноса рабочей станции за пределы корпоративной сети, сохранение всех данных перехвата. Автоматическое восстановление связи с серверной частью системы;

– возможность настройки автономного режима работы модуля;

Система должна отслеживать и отображать статистику по состоянию модулей контроля рабочих станций:

– поступление данных на сервер от каждого модуля,

– пользователей, контролируемых модулем;

– подключенные внешние устройства

– типы перехватываемых данных (протоколов).

Данные статистики должны быть доступны для экспорта.

2.3 Требования к перехвату HTTP-трафика, переданного через прокси-сервера

Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервера должен обеспечивать:

– возможность перехвата и фильтрации данных;

– возможность блокирования передачи исходящих сообщений по протоколу HTTP(S) на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных.

2.4 Требования к перехвату электронной почты, переданной через почтовые сервера

Система должна поддерживать интеграцию с почтовыми серверами, развернутыми на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного обеспечения, обеспечивающего перехват всех почтовых сообщений, переданных и полученных с помощью почтовых серверов по протоколам POP3, SMTP, IMAP и MAPI.

2.5 Требования к функциям хранения и обработки данных

В части хранения и обработки данных система должна обеспечивать:

– хранение всех перехватываемых данных вне зависимости от настроек политик безопасности, настроенных средствами системы;

– возможность централизованного хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL, MySQL (на выбор);

– возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз. Поисковые операции выполняются по всем базам данных в группе. Для событий запуска ротации можно настроить выполнение скриптов (перед и/или после ротации);

– поддержка работы с базами данных, расположенных на разных серверах;

– возможность настройки правил записи данных в базы для регуляции, в какую базу или группу баз записывать информацию в зависимости от типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутной информации;

– возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно;

– возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;

– защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;

– возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;

– возможность настройки расписания для репликации данных;

– возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;

– при переполнении очереди репликации сервер блокирует прием новых данных;

– отображение статистики репликации данных;

– возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;

– возможность сохранения файловых объектов большого размера на диск сервера, а не в базу. В базу данных при этом помещаются относительные пути к файлам;

– возможность настройки длительности хранения информации в базе данных в группе ротации, в том числе установки различной длительности хранения для различных типов данных (например, хранить почтовую переписку за последние 60 дней, а переписку через мессенджеры – за последние 30 дней);

– возможность очистки базы данных вручную через Консоль администратора;

– возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);

– возможность архивирования баз данных с последующим подключением к системе для осуществления поиска в них критичной информации;

– параллельную обработку данных, перехваченных по различным каналам передачи информации;

– настройку резервного хранилища модуля контроля рабочих станций в части ограничения размера и максимального периода хранения информации;

– настройку максимальной скорости передачи перехваченных данных с рабочих станций модулем контроля на сервер;

– асинхронный поиск по перехваченным данным (отображение результатов должно выполняться по мере их получения).

– возможность выборочного удаления пользователем перехваченной информации.

2.6 Требования к поддерживаемым форматам файлов

Система должна поддерживать обработку файлов следующих форматов:

– Adobe Acrobat (*.pdf)
– Ami Pro (*.sam)
– Ansi Text (*.txt)
– ASCII Text
– ASF (метаданные) (*.asf)
– CSV (Comma-separated values) (*.csv)
– DBF (*.dbf)
– DjVu
– DWG
– DXF
– EBCDIC
– EML files (электронные письма, сохраненные Outlook Express) (*.eml)
– Enhanced Metafile Format (*.emf)
– Eudora MBX файлы сообщений (*.mbx)
– Flash (*.swf)
– GZIP (*.gz)
– HTML (*.htm, *.html)
– JPEG (метаданные) (*.jpg)
– Lotus 1-2-3 (*.wk?, *.123)
– MBOX архивы электронных писем (включая Thunderbird) (*.mbx)
– MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht)
– Microsoft Access (*.mdb)
– Microsoft Access 2007 (*.accdb)
– Microsoft Document Imaging (*.mdi)
– Microsoft Excel (*.xls)
– Microsoft Excel 2003 XML (*.xml)
– Microsoft Excel 2007 (*.xlsx)
– Microsoft Open XML Paper Specification (*.oxps)
– Microsoft Outlook (OST)
– Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx)
– Microsoft PowerPoint (*.ppt)
– Microsoft Rich Text Format (*.rtf)
– Microsoft Searchable Tiff (*.tiff)
– Microsoft Word 2003 XML (*.xml)
– Microsoft Word 2007 (*.docx)
– Microsoft Word for DOS (*.doc)
– Microsoft Word for Windows (*.doc)
– Microsoft Works (*.wks)
– MIME-сообщения
– MP3 (метаданные) (*.mp3)
– MSG files (электронные письма, сохраненные Outlook) (*.msg)
– Multimate Advantage II (*.dox)
– Multimate version 4 (*.doc)
– OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений)
– OST (внутренний формат Microsoft Outlook)
– Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)

- TAR (*.tar)
- TIFF (*.tif)
- TNEF (winmail.dat)
- Treepad HJT (*.hjt)
- Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)
- Windows Metafile Format (*.wmf)
- WMA видео (метаданные) (*.wma)
- WMV видео (метаданные) (*.wmv)
- WordPerfect (5.0 и выше) (*.wpd, *.wpf)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordStar 2000
- WordStar версий 1, 2, 3, 4, 5, 6 (*.ws)
- Write (*.wri)
- XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf)
- XML Paper Specification (*.xps)
- XSL
- XyWrite
- ZIP (*.zip)

Кроме того, система должна обеспечивать распознавание и анализ текстовой информации в файлах графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR). Должна поддерживаться возможность выбора между встроенным и сторонним средствами распознавания.

2.7 Требования к возможностям управления пользователями

В системе должно быть обеспечено следующее:

- создание внутренних профилей (карточек) пользователей, содержащих всю идентификационную информацию пользователей локальной сети;
- интеграция с Active Directory (возможность импорта всех идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя; возможность автоматического создания (удаления) профилей пользователей при добавлении (удалении) записей в (из) Active Directory, автоматическое создание карточек при обнаружении ранее не известной пользовательской информации, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями с возможностью настройки расписания синхронизации);
- возможность выборочной интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;
- возможность автоматической привязки идентификационных данных пользователя, отсутствующих в Active Directory (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя;
- возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей (например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании);
- возможность создания и редактирования пользовательских карточек;
- возможность отображения пользовательских карточек как в виде линейного списка, так и с разбивкой на группы и подгруппы на основании информации из Active Directory (с учетом Organizational Units), либо на основании задаваемых параметров в карточках пользователей (произвольная группировка по организациям/отделам);
- аутентификация пользователей, работающих с системой, на основании их учетных записей Windows и на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);

– возможность разграничения прав доступа к системе и ее компонентам для различных пользователей с назначением ролей (например, «системный администратор» - доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения» - доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности» - доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) на основе аутентификации пользователей;

– политика сложности и срока действия паролей в режиме внутренней аутентификации;

– возможность отправки администратору уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения и т.д.);

– ведение журнала (лога) действий пользователей, работающих с системой.

3. Требования к перечню контролируемых каналов утечки

3.1 Требования к контролю электронной почты

Система должна обеспечивать контроль отправки информации посредством электронной почты, включая следующие возможности:

– перехват почтовых сообщений для нешифрованных и шифрованных (SSL) протоколов – IMAP, POP3, SMTP, MAPI плюс шифрованные аналоги;

– перехват почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME с автоматической расшифровкой содержимого письма;

– перехват почтовых сообщений путем интеграции с почтовыми серверами (на базе Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail и др.) по протоколам IMAP, POP3, SMTP (на выбор);

– перехват почтовых сообщений между Microsoft Outlook и Microsoft Exchange Server по протоколу MAPI (в том числе с использованием шифрования) путем интеграции с Microsoft Outlook;

– перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);

– перехват и анализ файлов-вложений почтовых сообщений;

– автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– блокировка исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений;

– возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;

– возможность поиска по тексту и атрибутам почтовых сообщений и файлов, переданных по почте.

3.2 Требования к контролю IM-клиентов

Система должна обеспечивать контроль отправки информации посредством IM-клиентов, включая следующие возможности:

– перехват сообщений и файлов посредством зеркалирования трафика на сетевом коммутаторе (для протоколов MRA, OSCAR, XMPP, YMSG, не использующих шифрование);

– возможность перехвата текстовых сообщений модулями, установленными на рабочие станции пользователей (Google Hangouts, Microsoft Lync, MRA, OSCAR, SIP, Skype, Slack, Telegram, Viber, WhatsApp, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);

– возможность перехвата файлов, отправляемых с рабочих станций (Microsoft Lync, MRA, OSCAR, Skype, Slack, Telegram, Viber, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);

– возможность перехвата голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber и по протоколу SIP с сохранением разговоров;

– возможность распознавания (перевода в текстовый формат) голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber и SIP;

– возможность воспроизведения сохраненных разговоров Telegram, Skype, Viber, Microsoft Lync и SIP;

– возможность ограничения перехвата по отдельным учетным записям пользователей;

– автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через IM-клиенты.

3.3 Требования к контролю HTTP-протокола

Система должна обеспечивать контроль отправки информации по HTTP-протоколу, включая:

– возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола HTTP);

– возможность перехвата посредством интеграции с прокси-серверами по протоколу ICAP (для протоколов HTTP и HTTPS);

– возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов HTTP и HTTPS);

– возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;

– возможность создания и гибкой настройки фильтров для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователем;

– возможность настройки фильтрации перехвата данных по MIME-типам;

– перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;

– перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;

– перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);

– перехват сообщений, переданных в веб-клиентах ICQ и Skype ;

– перехват и анализ поисковых запросов пользователя;

– сохранение адресов всех страниц (URL), посещенных пользователем;

– автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);

– возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов определенного содержания (HTTP и HTTPS);

– контроль браузер-активности (посещения веб-сайтов с помощью веб-браузера): фиксация переходов между страницами веб-сайтов и ведение комплексной статистики времени, проведенного на различных веб-ресурсах.

3.4 Требования к контролю FTP-протокола

Система должна обеспечивать контроль информации, передаваемой по протоколу FTP, включая возможности:

– перехвата файлов, загруженных или переданных по простому FTP-соединению, а также переданных по зашифрованному SSL-соединению;

– возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола FTP);

– возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов FTP и FTPS);

– возможность настройки ограничения по размеру перехватываемых файлов;

– автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S).

3.5 Требования к контролю принтеров

Система должна обеспечивать контроль информации, отправляемой на печать, включая:

– возможность перехвата документов, отправляемых на сетевые и локальные принтеры (в том числе подключенные к COM-, LPT-портам);

– возможность перехвата печати в XPS-формат;

– возможность настройки исключений из перехвата по отдельным принтерам;

– возможность ограничения перехвата печати по количеству страниц и по размеру документа;

– возможность исключения процессов для модуля перехвата печати на принтерах.

– извлечение и анализ текста отправленных на печать документов;

– автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность поиска по тексту и атрибутам отправленных на печать файлов;

– сохранение перехваченного текста (PDF и HTML-формат).

3.6 Требования к контролю подключенных устройств и внешних накопителей информации

Система должна обеспечивать контроль информации, отправляемой на внешние носители, включая:

– теневое копирование файлов, отправляемых на внешние накопители информации (съемные жесткие диски, карты памяти, съемные накопители, CD/DVD и флоппи-диски);

– возможность настройки исключений из теневого копирования по размеру и расширению файлов;

– возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

– возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

– возможность настройки исключений из теневого копирования для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);

– контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);

– управление правами записи на внешние накопители информации с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;

– возможность контроля копирования информации на внешние накопители информации как в локальных, так и терминальных пользовательских сессиях;

– аудит событий копирования файлов на внешние накопители: должно фиксироваться имя файла, пользователь, дата, время и данные устройства;

– контроль доступа и аудит использования внешних устройств любого типа, подключаемых к рабочей станции, по набору параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);

– автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность поиска по тексту и атрибутам файлов, отправленных на внешние накопители информации.

3.7 Требования к контролю локальных сетевых ресурсов

Система должна обеспечивать контроль информации, отправляемой на локальные сетевые ресурсы, включая следующие возможности:

– теневое копирование файлов, отправляемых на сетевые ресурсы;

– возможность настройки исключений из теневого копирования по расширениям файлов;

– возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

– возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

– контроль доступа к сетевым ресурсам с возможностью запрета доступа для определенных пользователей;

– управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;

– возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;

– автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– аудит событий копирования файлов на локальные сетевые ресурсы: фиксация имени файла, пользователь, дата, время и сетевой путь к ресурсу;

– возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов.

3.8 Требования к контролю облачных хранилищ (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск)

Система должна обеспечивать контроль использования облачных хранилищ, в том числе:

– теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;

– возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;

– возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

– возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

– контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;

– управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;

– автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– аудит событий отправки файлов в облачные хранилища с фиксацией имени файла, имени пользователя, даты, времени и имени облачного сервиса хранения;

– возможность поиска по тексту и атрибутам отправленных файлов.

4. Требования к возможностям мониторинга действий пользователей на ПК

4.1 Требования к функции снятия скриншотов

Система должна выполнять сохранение снимков рабочего стола пользователей и обеспечивать:

– возможность снятия скриншотов с заданным интервалом с точностью до секунды;

– возможность снятия скриншотов при смене активного окна и смене вкладки браузера, запуске нового процесса;

– возможность снятия скриншотов при срабатывании правила блокировки;
– возможность снятия скриншотов при нажатии клавиши Print Screen;
– возможность настройки качества скриншотов (в т.ч. сохранения в черно-белом формате);
– возможность настройки размера скриншотов (в процентах от оригинала);
– возможность настройки формата скриншотов (JPEG, PNG);
– сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);
– возможность отключения захвата снимков при простое рабочей станции;
– возможность экспорта снимков экранов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;
– возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
– возможность сохранения скриншотов нескольких пользователей за выбранный интервал дат в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
– при просмотре скриншота отображается «watermark» с названием компьютера и именем пользователя.

4.2 Требования к функции сбора статистики по активности ПК

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции:
– ведение статистики по времени работы и простоя (отсутствия действий пользователя) ПК с представлением собранной информации в виде графика;
– ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
– возможность настройки исключений отдельных процессов из мониторинга;
– возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в виде PDF-файла;
– возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу.

4.3 Требования к контролю буфера обмена

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции:
– теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
– возможность ограничения максимального объема текста, перехватываемого из буфера обмена;
– автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
– возможность поиска по тексту, помещаемому пользователями в буфер обмена.

4.4 Требования к функциям кейлоггера

Система должна поддерживать:
– регистрацию нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных клавиш (Shift, Enter, Backspace и т.п.);
– автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

– возможность поиска по тексту, вводимому пользователями с клавиатуры.

4.5 Аудиомониторинг

Система должна обеспечивать возможность прослушивания звуковых потоков с рабочей станции, в том числе:

– подключение к микрофонам контролируемых рабочих станций с возможность прослушивания аудиопотока в режиме реального времени;

– прослушивание микрофонов нескольких пользователей одновременно;

– автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;

– запись вручную;

– возможность сохранения записей нескольких пользователей одновременно;

– возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.6 Видеомониторинг

Система должна поддерживать:

– подключение к монитору компьютера пользователя и просмотра изображения рабочего стола в режиме реального времени;

– мониторинг рабочих столов нескольких пользователей одновременно;

– возможность вывода окна просмотра на отдельный экран;

– автоматическая запись видеоизображения рабочего стола и подключенной веб-камеры по расписанию;

– запись вручную;

– возможность сохранения записей нескольких пользователей одновременно;

– возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.7 Требования к контролю файловых систем:

Контроль файловых систем должен позволять:

– формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;

– автоматическое сканирование дисков контролируемых компьютеров на предмет наличия определенных документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;

– возможность выбора компьютеров и пользователей, чьи файловые системы будут контролироваться;

– гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;

– возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций;

– возможность удаленного поиска документов в файловых системах контролируемых рабочих станций на основе атрибутов файлов и значения их хеш-функций.

5. Требования к методам анализа перехваченной информации и процедурам реагирования на инциденты безопасности

Система должна обеспечивать следующие функциональные возможности при работе с политиками безопасности:

– автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента); уведомление содержит общую информацию об инциденте (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента), а также ссылку на открытие соответствующего инцидента в пользовательской консоли;

– возможность указания групп Active Directory, к которым могут быть применены политики безопасности;

– возможность добавлять/исключать/редактировать категории и уровни риска инцидентов сервера безопасности для автоматического расчёта показателей уровней риска пользователей;

– возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.);

– возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли (с индивидуальным выделением просмотренных/непросмотренных инцидентов для каждого офицера безопасности, работающего с системой);

– при просмотре информации об инциденте в клиентской консоли доступна следующая информация:

- пользователь, допустивший нарушение;
- дата и время инцидента;
- показатель присвоенного уровня риска;
- тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.);
- содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности;
- другая дополнительная информация.

– возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);

– возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые (непросмотренные) инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);

– возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);

– возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);

– возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;

– возможность экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);

– возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;

– ведение журнала (лога) действий офицера безопасности.

При анализе информации должны быть реализованы следующие возможности (аналитические возможности системы должны быть одинаковы для всех поддерживаемых языков анализируемой информации – включая анализ информации на английском, арабском, белорусском, испанском, казахском, китайском, корейском, немецком, русском и других языках):

Контентный анализ:

– поиск по словам и словосочетаниям с учетом морфологии (возможность отключения), расстояния между словами и порядка слов, транслитерации кириллических символов латинскими, а также с возможностью нечеткого поиска (для поиска ключевых слов, в т.ч. написанных с ошибками и опечатками);

– поддержка регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;

– поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок/регулярных выражений в словарях, с возможностью настройки порога

срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре);

– поиск документов с умышленно измененным расширением;

– поиск документов, защищенных паролем;

– цифровые отпечатки документов: возможность создания цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента совпадения);

– цифровые отпечатки баз данных: возможность настройки подключения системы к базе данных, содержащей конфиденциальную информацию, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой БД (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»). Создание и обновление цифровых отпечатков баз данных должно осуществляться без промежуточных действий (таких как выгрузка базы данных в файл-источник цифрового отпечатка). При внесении изменений в базу данных система должна автоматически обновлять соответствующие цифровые отпечатки.

– комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ».

– поиск данных по DNS-имени и SID компьютера, по имени и SID домена среди данных, перехваченных агентами.

– поиск информации по группам Active Directory.

Анализ по атрибутам

– анализ по атрибутам пользовательских документов, таким как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «размер» и пр.;

– анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных.

– анализ атрибутов процессов: имя исполняющего файла, полный путь к файлу, заголовок окна процесса.

Статистический анализ

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем электронным письмам (например, «пользователь получил более 10 писем за час» или «пользователь отправил менее 20 писем за день» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем файлам (например, «пользователь получил более 10 файлов за час» или «пользователь отправил более 20 файлов за день» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по переписке пользователя в IM-клиентах (например, «пользователь провел более 10 сессий переписки за день» или «пользователь отправил более 100 сообщений за день» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по голосовым переговорам в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по посещенным пользователем URL (например, «пользователь посетил более 100 URL за день», «пользователь посетил более 1000 URL за неделю» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по поисковым запросам пользователя (например, «пользователь отправил более 100 поисковых запросов в период с 13:00 до 15:00» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по данным, отправленным пользователем на печать (например,

«пользователь распечатал более 10 документов за день» или «пользователь распечатал более 1000 страниц за неделю» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности/простоя ПК (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени работы пользователя с определенными приложениями (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);

– возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

Событийный анализ

Возможность настройки автоматических уведомлений в следующих случаях:

– выявления факта запуска (завершения) пользователем определенного приложения;

– обнаружения пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);

– копирования файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;

– подключения и использования на контролируемых рабочих станциях устройств с определенными параметрами;

– блокирования пересылки данных по SMTP, HTTP, MAPI;

– посещение определенных web-ресурсов;

– обнаружения конфиденциальных файлов на компьютерных дисках пользователей;

– выявления факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения).

Анализ рисков

Возможность дополнить политики безопасности следующим функционалом:

– формировать модели поведения сотрудников и задавать им соответствующий уровень риска;

– информировать специалистов отдела безопасности об уровне риска и об инцидентах политик безопасности, которые вызвали изменения уровней риска;

– отслеживать изменения в поведении сотрудников в режиме реального времени.

Независимо от используемого типа анализа, система должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных данных (для выявления фактов нарушения вновь созданной политики безопасности в прошлом за весь период наблюдения).

6. Организация документов при проведении расследований

Система должна предусматривать специальный модуль для организации информации и документации для проведения расследований (типа «центр расследований»), который должен обеспечивать следующие возможности:

- в целях сбора доказательств по инцидентам безопасности -- создание документа (дела), который может включать в себя:

– информацию об инциденте;

– перечень вовлеченных лиц и их реквизиты;

– перечень проводимых (проведенных) мероприятий по расследованию инцидента и их результаты;

– выводы по результатам расследований;

– материалы расследований – внутренние документы (результаты перехвата) системы;

– реквизиты внутренних документов: тип данных, локальный пользователь, удаленный пользователь, дата перехвата, размер документа;

– материалы расследований – внешние документы;
– внешние документы, содержащие аналитические записки, рапорты и т.п.

- в целях комплексного аудита результатов перехвата обеспечивать функции:

– просмотр содержания документов в расширенном виде напрямую из дела;
– фильтрацию документов при просмотре в деле;
– представление включенных в дело документов в режимах просмотра карточки, список;
– возможность экспорта дела в форматы *.pdf, *.xps.
– возможность распечатки дела на принтере.

- в целях контроля за внесением изменений в дело наличие журнала событий, включающего в себя информацию о всех вносимых правках:

– имя пользователя, который совершил операцию в деле;
– совершенное действие;
– дату и время совершенного действия;
– прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.

- в целях упрощения работы лиц, ведущих расследование обеспечивать:

– ведение списка дел;
– возможность сортировки дел в группы;
– возможность создания групп и подгрупп с количество уровней иерархии не менее 20;
– возможность переноса дел из группы в группу простым перетаскиванием «мышкой»;
– возможность переноса подгрупп из группы в группу простым перетаскиванием «мышкой»;
– возможность удаления дел и групп;
– возможность исправления дел;
– возможность просмотра: всех дел, только открытых дел, только закрытых дел;
– возможность глубокой пользовательской настройки просмотра дел: всех дел за определенный период; дел, открытых в определенный период; дел, закрытых в определенный период;
– возможность закрепления и открепления поля списка дел;
– возможность переноса поля списка дел к любой стороне окна программы.

Система также должна обеспечивать возможность удобного присоединения документов к делу в модуле типа «центр расследований» из других модулей системы: например, через контекстное меню.

7. Требования к отчетности

Все перехваченные данные должны представляться в форме отчетов следующих видов:

Отчет об активности пользователя

- Вкладка «Дневная активность» на временной сетке с шагом в 1 час должна содержать:

– информацию о количестве отправленных и полученных пользователем писем;
– информацию о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;
– информацию о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах;
– информацию о количестве посещенных URL и отправленных поисковых запросов;
– информацию о количестве сделанных системой снимков экрана рабочего стола пользователя;
– информацию о времени работы/простоя компьютера пользователя, детальную статистику активности приложений и данные о процентном соотношении времени работы в различных приложениях;
– информацию о количестве документов, помещенных в буфер обмена;
– информацию о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;
– информацию о количестве символов, введенных пользователем с клавиатуры.

Вкладка должна быть интерактивная и динамическая, чтобы позволять осуществлять переход по ссылкам непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок.

Должна быть обеспечена возможность экспорта дневной активности во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к перехваченным данным в веб-браузере, а также с возможностью сохранения выбора ассоциированных просмотривщиков для разных типов документов в расширенных настройках.

- Вкладка «Статистика по активности»

Система должна представлять данные, собранные по определенному пользователю за конкретный интервал времени, в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов).

Графики по типам информации должны поддерживать интерактивность и динамичность, поддерживать возможность перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов.

Необходимо предусмотреть возможность сохранения статистики во внешний файл формата PDF и XPS.

- Вкладка «Взаимосвязи»

Система должна обладать возможностью графического отображения взаимосвязей пользователя (в виде графа или таблицы) на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь обменивался какой-либо информацией в течение выбранного интервала времени.

Должна быть обеспечена поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.

Возможность просмотра взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.

Возможность выбора масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).

Возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.

Поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

Отчет по пользователям

Система должна реализовывать возможность построения сводного интерактивного отчета по определенному пользователю за все время наблюдения (или за выбранный интервал времени), включающего следующую информацию:

- статистика перехвата данных, в том числе

– количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;

– количество посещенных сайтов и поисковых запросов;

– количество файлов, переданных/принятых по FTP;

– количество распечатанных документов и страниц;

– количество операций копирования в буфер обмена;

– количество снятых скриншотов;

– количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;

– количество нажатых клавиш клавиатуры.

- информация об активности пользователя за компьютером, в том числе

– общее время активной работы пользователя за ПК;

– среднесуточное время активной работы пользователя за ПК;

– общее время простоя ПК;

– среднесуточное время простоя ПК;

– общее время присутствия сотрудника на работе;

– среднесуточное время присутствия сотрудника на работе;

– среднее время начала работы;
– среднее время окончания работы;
– общее количество рабочих дней;
– календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой);
– гистограмма по времени активности/простоя компьютера пользователя за каждый день.

- информация об активности приложений на компьютере пользователя, в том числе

– процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы);
– полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них.

- информация о браузер-активности, в том числе

– рейтинг посещенных веб-ресурсов;
– хронология активности в веб-браузере.

- информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.

Необходимо предусмотреть возможность пакетного сохранения отчетов для групп пользователей с предварительной настройкой единой формы отчета.

ТОП-отчет по пользователям

Система должна обеспечивать создание сводных интерактивных отчетов по всем контролируемым каналам передачи данных за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, наиболее активно использующих этот канал.

Система должна содержать возможность построения ТОП-отчета для сотрудников, входящих в группы пользователей системы либо в группы пользователей Active Directory.

Необходимо предусмотреть возможность построения сводных отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз.

При создании отчетов должна быть обеспечена возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов, то есть «Браузер активность: количество посещенных сайтов» и «Браузер активность: время проведенное на сайте».

тчет по политикам безопасности

Система должна обеспечивать возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, заданных в модуле Политики безопасности.

При этом система должна обеспечивать просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр итогового количества срабатываний по каждому правилу в отдельности и по всем существующим правилам безопасности.

Сводный отчет по пользователям

Система должна предусматривать возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей.

Также необходимо обеспечить просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики для выбранных статистических показателей.

8. Мониторинг работоспособности системы

Система должна поддерживать:
– ведение журнала событий серверных компонентов системы;

– просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;

– фильтрацию событий в журнале по рабочей станции, серверному компоненту, уровню, дате;

– выбор определенных рабочих станций для ведения мониторинга;

– автоматическое уведомление администратора системы о новых событиях серверных компонентов через консоль администратора и по почте;

– настройку правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

Систем должна фиксировать сведения о всех наиболее существенных событиях в работе серверных компонентов в журнале операционной системы рабочей станции, на которой они установлены.

9. Прочие требования

В процессе своего функционирования система не должна оказывать негативного влияния на функционирование прикладных ИС Заказчика.

Масштабируемость системы

В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы:

– возможность установки нескольких серверов перехвата данных для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;

– возможность установки нескольких серверов контроля агентов для контроля разных сегментов сети или разных групп компьютеров;

– возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;

– возможность установки нескольких серверов индексирования для оптимизации и распределения нагрузки на сервер и базу данных;

– возможность установки нескольких серверов обработки почты для работы с несколькими почтовыми серверами (MS Exchange, IBM Lotus Domino и др.).

Ориентация работы всех компонентов системы на многопоточность

Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах. С помощью добавочного модуля распознавания ABBYY должна существовать возможность распознавания одновременно нескольких PDF-документов.

Удобство администрирования

Система должна обеспечивать следующие функции, повышающие эффективность администрирования программы:

– Централизованное управление компонентами системы с использованием шифрования из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ).

– Возможность централизованного подключения и настройки хранилищ информации, а также создания резервной копии конфигурации всех серверных компонентов с поддержкой последующего восстановления настроек серверов через консоль администратора.

– Возможность автоматического переподключения к серверу при разрыве соединения с консолью пользователя.

– Возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности;

– Возможность отключения автоматического управления системным брандмауэром.

– Возможность при настройке профилей для агентов добавлять компьютер в профиль из схемы агентов, а также копировать/перемещать объекты между профилями.

– Автоматическая фиксация пользователей, которые проводят авторизацию или отклонении сервера-компонента на центральном сервере.

Политика лицензирования ПО

Система должна лицензироваться в соответствии с количеством контролируемых пользователей (500 лицензий для рабочих мест, включая 500 лицензий модуля распознавания изображений ABBYY, 600 лицензий на перехват сервером обработки корпоративной почты). При этом недопустимо использование жесткой привязки лицензии к конкретным рабочим станциям или

пользователям. Количество приобретенных лицензий должно определять только количество одновременно контролируемых пользователей, при этом сам список контролируемых может быстро и гибко изменяться в случае необходимости (например, при наличии 100 пользователей в сети и только 50 лицензий – возможность контролировать выборочно сначала одних пользователей, затем других; при этом переназначение лицензионных слотов должно быть возможно не реже 1 раза в сутки).

Система должна предусматривать возможность покомпонентной поставки, т.е. выбора типов контролируемых данных и отключения неиспользуемого функционала на уровне лицензии. Кроме того, лицензии должны быть бессрочны, в состав системы лицензирования должен быть включен 1 год техподдержки, а также внедрение и настройка Системы.

Руководитель _____ /_____/
(подпись) (расшифровка подписи)

Приложение № 2
к Заявке

АНКЕТА УЧАСТНИКА*

1. Для Участника: 1.1. Юридического лица – полное наименование организации и ее организационно-правовая форма. 1.2. Физического лица, в том числе зарегистрированного в качестве индивидуального предпринимателя – фамилия, имя, отчество.	
2. Для Участника: 2.1. Юридического лица – место нахождения (юридический адрес) 2.2. Индивидуального предпринимателя – серия, номер и дата выдачи свидетельства о государственной регистрации, адрес регистрации 2.3. Физического лица – паспортные данные (серия и номер паспорта, кем и когда выдан, код подразделения, адрес регистрации)	
3. Для Участника: 3.1. Юридического лица – ИНН, КПП, ОГРН, ОКПО 3.2. Индивидуального предпринимателя – ИНН, ОГРНИП 3.3. Физического лица – ИНН, СНИЛС	
4. Фактический (почтовый) адрес Участника	
Страна	
Адрес	
Телефон	
Факс	
5. Банковские реквизиты (может быть несколько):	
5.1. Наименование обслуживающего банка	
5.2. Расчетный счет	
5.3. Корреспондентский счет	
5.4. Код БИК	
6. Фамилия, имя, отчество генерального директора (лица имеющего право подписи без доверенности), номер телефона	

Мы, нижеподписавшиеся, заверяем правильность всех данных, указанных в анкете.

_____ _____ /_____/

(должность) (подпись) (ФИО)

М.П.

** Анкета участника размещается на электронной площадке в формате Word.*

Приложение № 3
к Документации

СОГЛАСИЕ
на обработку персональных данных Участника
(представителя Участника)

Я, _____ ,
(фамилия, имя, отчество)

паспорт серии _____ , номер _____ , выдан _____
(дата выдачи)

_____ ,
(наименование органа, выдавшего паспорт)

_____ ,
(адрес места регистрации)

в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ выражаю автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (далее – Аналитический центр при Правительстве Российской Федерации), зарегистрированному по адресу: Российская Федерация, г. Москва, проспект Академика Сахарова, д.12, согласие на обработку моих персональных данных.

Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя и отчество;

дата и место рождения;

паспортные данные;

адрес места регистрации;

биометрические персональные данные (фотография).

Целью обработки персональных данных является проявление должной осмотрительности при выборе контрагента для заключения договора и минимизации (исключения) налоговых и репутационных рисков при осуществлении делового сотрудничества с ним.

Действия с моими персональными данными могут включать в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка моих персональных данных может осуществляться как с применением средств автоматизации, так и без применения таких средств.

Настоящее согласие предоставляется на срок подготовки и действия договора с Аналитическим центром при Правительстве Российской Федерации.

Я осведомлён о том, что настоящее согласие может быть отозвано мной в любое время на основании моего письменного заявления.

«__» _____ 20__ г. _____

Приложение № 3
к Документации

ПРОЕКТ

СУБЛИЦЕНЗИОННЫЙ ДОГОВОР № _____

г. Москва **«__» _____ 2020 г.**

Автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации», именуемая в дальнейшем СУБЛИЦЕНЗИАТ, в лице _____, действующего на основании_____ с одной стороны, и _____, именуемое в дальнейшем СУБЛИЦЕНЗИАР, в лице _____, действующего на основании _____, с другой стороны, совместно именуемые Стороны, заключили настоящий договор (далее - Договор) о нижеследующем:

1. ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В ДОГОВОРЕ

ПРАВООБЛАДАТЕЛЬ – юридическое или физическое лицо, обладающее исключительными правами на программы ЭВМ и базы данных.

ПРОДУКТ – экземпляр лицензионного программного обеспечения для ЭВМ и базы данных, а также любые носители с ними, документация и иные принадлежности, которые необходимы для использования программ для ЭВМ и баз данных КОНЕЧНЫМИ ПОЛЬЗОВАТЕЛЯМИ.

СУБЛИЦЕНЗИАР – юридическое лицо, обладающее правами на распространение и воспроизведение ПРОДУКТОВ, а также на передачу прав на распространение и использование ПРОДУКТОВ на законном основании.

СУБЛИЦЕНЗИАТ - КОНЕЧНЫЙ ПОЛЬЗОВАТЕЛЬ – пользователь (потребитель) ПРОДУКТОВ, непосредственно воспроизводящий ПРОДУКТ на компьютере, сервере путем инсталляции и запуска в соответствии с правилами лицензионного использования конкретного ПРОДУКТА, установленными соответствующими ПРАВООБЛАДАТЕЛЯМИ.

2. ПРЕДМЕТ ДОГОВОРА

2.1. СУБЛИЦЕНЗИАР, имея соответствующие полномочия от ПРАВООБЛАДАТЕЛЕЙ (сертификат), и действуя в соответствии с требованием ст.ст. 1235-1238, 1286 Гражданского кодекса Российской Федерации, обязуется поставить СУБЛИЦЕНЗИАТУ неисключительные права на использование ПРОДУКТА (простая неисключительная лицензия) в соответствии со Спецификацией (Приложение № 1 к Договору).

2.2. Право на использование ПРОДУКТА, предоставляемое (передаваемое) СУБЛИЦЕНЗИАТУ в соответствии с Договором, включает использование следующими способами: неисключительное право на воспроизведение ПРОДУКТА в качестве конечного пользователя, ограниченное правом инсталляции, копирования и запуска ПРОДУКТА в соответствии с лицензионным соглашением для конечного пользователя, подтверждаемого СУБЛИЦЕНЗИАТОМ при установке ПРОДУКТА, а также осуществление технической поддержки СУБЛИЦЕНЗИАТУ на следующих условиях (телефонная и инцидентная поддержка 12х5 (с понедельника по пятницу, с 10 утра до 10 вечера); неограниченное количество запросов поддержки; удаленная поддержка; онлайн-доступ к документации и техническим ресурсам; форум; обновления ПРОДУКТА в течение 12 месяцев.

2.3 Наименование ПРОДУКТА, права на распространение и использование которых передаются от СУБЛИЦЕНЗИАРА к СУБЛИЦЕНЗИАТУ, размер лицензионного платежа (вознаграждение) указываются в Спецификации (Приложение № 1 к Договору), счетах и Актах передачи прав, которые подписываются Сторонами при передаче прав.

2.4. Срок передачи ПРОДУКТА: в течение 7 (Семи) рабочих дней с даты заключения Договора.

2.5. Срок, на который передаются неисключительные права: бессрочно.

2.6. Территория, на которой допускается использование СУБЛИЦЕНЗИАТОМ ПРОДУКТОМ устанавливается как вся территория страны СУБЛИЦЕНЗИАТА.

2.6. Договор заключен Сторонами по итогам проведения запроса цен в электронной форме.

Протокол № _____ от _____ 2020 г.

3. ЛИЦЕНЗИОННЫЕ ПЛАТЕЖИ И ПОРЯДОК РАСЧЕТОВ

3.1. Цена неисключительных прав, передаваемых СУБЛИЦЕНЗИАТУ по Договору, составляет _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

3.2. Цена Договора включает в себя все обязательные платежи и расходы, связанные с исполнением Договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

3.3. Оплата производится СУБЛИЦЕНЗИАТОМ по факту предоставления ПРОДУКТОВ, в течение 10 (Десяти) рабочих дней с даты получения счета, выставленного на основании подписанного Сторонами Акта передачи прав.

3.4. Передача неисключительных прав по Договору от СУБЛИЦЕНЗИАРА к СУБЛИЦЕНЗИАТУ оформляется Актом передачи прав, который подписывается Сторонами в течение 7 (Семи) рабочих дней с момента активации лицензионного ключа.

Без Договора Акт передачи прав не имеет юридической силы.

3.5. В течение 7 (Семи) рабочих дней с даты заключения Договора СУБЛИЦЕНЗИАР обязан предоставить СУБЛИЦЕНЗИАТУ возможность пользования ПРОДУКТАМИ, права на использование которых передаются ему по Договору, включая предоставление необходимых ключей, паролей доступа и т.п.

3.6. Датой оплаты считается день списания денежных средств с расчетного счета СУБЛИЦЕНЗИАТА.

Датой получения документов считается дата их регистрации в системе документооборота СУБЛИЦЕНЗИАТА.

В первичных учетных документах указывается дата и номер Договора.

4. ПРАВА И ОБЯЗАННОСТИ СУБЛИЦЕНЗИАТА

4.1. СУБЛИЦЕНЗИАТ обязуется:

Выплатить СУБЛИЦЕНЗИАРУ вознаграждение в порядке и размерах, предусмотренных Договором.

Строго придерживаться и не нарушать правил лицензионного использования ПРОДУКТОВ.

Не совершать относительно ПРОДУКТОВ другие действия, нарушающие российские и международные нормы по авторскому праву и использованию программных средств.

5. ПРАВА И ОБЯЗАННОСТИ СУБЛИЦЕНЗИАРА

5.1. СУБЛИЦЕНЗИАР обязуется:

Передать права СУБЛИЦЕНЗИАТУ на условиях, предусмотренных Договором.

Не совершать действия, противоречащие условиям Договора и наносящие ущерб СУБЛИЦЕНЗИАТУ.

5.2. СУБЛИЦЕНЗИАР дает согласие на осуществление Управлением делами Президента Российской Федерации (главным распорядителем средств федерального бюджета) и уполномоченными органами государственного финансового контроля проверок соблюдения порядка, целей и условий предоставления субсидий.

5.3. СУБЛИЦЕНЗИАР вправе в качестве первичных учетных документов использовать универсальный передаточный документ (УПД).

6. ПОРЯДОК ПЕРЕДАЧИ-ПРИЕМА ПРАВ

6.1. Права передаются СУБЛИЦЕНЗИАТУ в виде лицензионного ключа, представляющего собой буквенно-цифровую последовательность символов.

6.2. Способ передачи прав – в электронной форме, на электронную почту itm@ac.gov.ru.

6.3. При условии надлежащего выполнения СУБЛИЦЕНЗИАРОМ своих обязательств СУБЛИЦЕНЗИАТ в течение 7 (Семи) рабочих дней со дня получения Акта передачи прав подписывает Акт передачи прав и направляет его СУБЛИЦЕНЗИАРУ.

6.4. В случае отказа СУБЛИЦЕНЗИАТА от подписания Акта передачи прав СУБЛИЦЕНЗИАТ делает соответствующую отметку в Акте передачи прав или составляет акт с перечнем недостатков и сроков их устранения. СУБЛИЦЕНЗИАР обязан устранить недостатки в установленные СУБЛИЦЕНЗИАТОМ сроки.

После устранения замечаний СУБЛИЦЕНЗИАР осуществляет передачу права в порядке, предусмотренном п.п. 6.3. - 6.4. Договора.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Договор вступает в силу с даты подписания обеими Сторонами и действует до полного исполнения Сторонами своих обязательств.

7.2. Договор может быть расторгнут по взаимному соглашению Сторон или по вступившему в законную силу решению арбитражного суда.

7.3. СУБЛИЦЕНЗИАТ может расторгнуть Договор в одностороннем внесудебном порядке в случае невыполнения СУБЛИЦЕНЗИАРОМ условий Договора.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. За неисполнение или ненадлежащее исполнение своих обязательств по Договору Стороны несут ответственность, в соответствии с действующим законодательством Российской Федерации.

8.2. В случае просрочки исполнения СУБЛИЦЕНЗИАТОМ обязательства, предусмотренного Договором СУБЛИЦЕНЗИАР вправе потребовать уплату неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается Договором в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Банка России от не уплаченной в срок суммы.

8.3. СУБЛИЦЕНЗИАТ освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине СУБЛИЦЕНЗИАРА.

8.4. В случае невыполнения СУБЛИЦЕНЗИАРОМ предусмотренных Договором обязательств в установленные сроки, СУБЛИЦЕНЗИАТ вправе потребовать уплату пени в размере до 0,5% от цены неисключительных прав по Договору за каждый день просрочки.

Штрафы начисляются за неисполнение или ненадлежащее исполнение СУБЛИЦЕНЗИАРОМ обязательств, предусмотренных Договором, за исключением просрочки исполнения СУБЛИЦЕНЗИАРОМ обязательств, предусмотренных Договором, в размере до 10 % цены неисключительных прав по Договору.

При этом СУБЛИЦЕНЗИАТ из сумм, подлежащих выплате СУБЛИЦЕНЗИАРУ, вправе удерживать суммы штрафных санкций и иных санкций, которые СУБЛИЦЕНЗИАР обязан уплатить СУБЛИЦЕНЗИАТУ в соответствии с разделом 8 Договора за ненадлежащее исполнение условий Договора.

8.5. СУБЛИЦЕНЗИАР освобождается от уплаты пени, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине СУБЛИЦЕНЗИАТА.

9. КОНФИДЕНЦИАЛЬНОСТЬ

9.1. Условия Договора, дополнительных соглашений к нему и иная информация, полученная СУБЛИЦЕНЗИАРОМ в соответствии с Договором, конфиденциальны и не подлежат разглашению СУБЛИЦЕНЗИАРОМ.

10. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ.

10.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Договору в случае действия обстоятельств непреодолимой силы, прямо или косвенно препятствующих исполнению Договора, то есть таких обстоятельств, которые независимы от воли Сторон, не могли быть ими предвидены в момент заключения Договора и предотвращены разумными средствами при их наступлении.

10.2. Сторона, подвергшаяся действию таких обстоятельств, обязана немедленно в письменном виде уведомить другую Сторону о возникновении, виде и возможной продолжительности действия соответствующих обстоятельств.

10.3. Наступление обстоятельств, предусмотренных настоящей статьей, при условии соблюдения требований п. 10.2 Договора, продлевает срок исполнения договорных обязательств на период, который в целом соответствует сроку действия наступившего обстоятельства и разумному сроку для его устранения.

10.4. В случае, если обстоятельства, предусмотренные настоящей статьей, длятся более 2 (Двух) месяцев, Стороны проводят переговоры для определения альтернативных способов исполнения Договора.

11. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

11.1. В случае изменения учредительных документов, банковских реквизитов, адресов, Сторона, у которой происходят такие изменения, обязана известить другую Сторону в течение 5 (Пяти) дней с момента изменений, путем направления в ее адрес надлежащим образом оформленного уведомления, без заключения дополнительного соглашения.

11.2. Споры по Договору рассматриваются в претензионном порядке. Стороны устанавливают срок рассмотрения претензий – 15 (Пятнадцать) дней с момента их получения. В случае не достижения соглашения спор передается на рассмотрение в Арбитражный суд города Москвы.

11.3. Любые изменения и дополнения к Договору действительны лишь при условии, что они совершены в письменной форме и подписаны уполномоченными представителями Сторон

11.4. Во всем остальном, что не предусмотрено в Договоре, Стороны руководствуются действующим законодательством Российской Федерации

11.5. Договор составлен в 2-х (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

11.6. Приложение, указанное в настоящем Договоре и являющееся его неотъемлемой частью:

Приложение № 1 - Спецификация.

АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

СУБЛИЦЕНЗИАТ:
автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации»

Адрес: 107078, город Москва,
проспект Академика Сахарова, д. 12,
телефон: (495) 632-97-96
ОГРН 1157700000655
ИНН 7708244720
КПП 770801001
ОКПО 94194039
ОКТМО 45378000
Банковские реквизиты:
УФК по г. Москве (л/с 711В0011001)
Банк: ГУ Центрального Банка РФ по ЦФО
БИК 044525000
р/с 40501810345251000279

_____/ / **СУБЛИЦЕНЗИАР:** _____ / /

Приложение №1
к Договору № _____
от «_____» _____ 2020 г.

СПЕЦИФИКАЦИЯ

на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

№ п/п	Наименование	Кол-во лицензий, шт.	Цена за ед. руб., (без НДС)	Сумма в руб. (без НДС)
1	Лицензия на программное обеспечение «Falcongaze SecureTower» (контроль: MAIL; WEB; IM; FTP; USB; Printers; Desktop activity; Indexing), Стандартные версии	500	*	*
2	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер контроля агентов, Стандартные версии	1	*	*
3	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер обработки данных, Стандартные версии	1	*	*
4	Лицензия на программное обеспечение "Falcongaze SecureTower», сервер обработки почты, Стандартные версии	1	*	*
5	Лицензия на программное обеспечение «Falcongaze SecureTower», перехват сервером обработки почты (контроль e-mails), Стандартные версии	600	*	*
6	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания изображений, Стандартные версии	1	*	*
7	Лицензия на программное обеспечение «Falcongaze SecureTower», средство распознавания изображений ABBYY, Стандартные версии	500	*	*
8	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер расследований инцидентов, Стандартные версии	1	*	*
9	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер распознавания речи, Стандартные версии	1	*	*
10	Лицензия на программное обеспечение «Falcongaze SecureTower», сервер анализа рисков, Стандартные версии	1	*	*
Итого				*

Цена неисключительных прав, передаваемых СУБЛИЦЕНЗИАТУ по Договору, составляет _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

** Заполняется в соответствии с предложением победителя запроса цен в электронной форме*

Текст, выделенный курсивом, в заявке не воспроизводится.

Требования к функциональным возможностям программной системы

1. Требования к назначению программной системы

Программная система (далее - Система) должна обеспечивать решение следующих задач:

- мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов вычислительных сетей Заказчика конфиденциальной информации по следующим каналам:
  - электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги);
  - электронная почта, защищенная по стандарту S/MIME;
  - электронная почта, переданная через почтовые веб-службы (Gmail.com, Hotmail.com, Mail.ru, Rambler.ru, Yahoo.com, Yandex.ru и т.д.);
  - двунаправленный перехват сообщений в чатах, статусов, комментариев к публикациям и на форумах социальных сетей: Facebook, Twitter, ВКонтакте, Одноклассники;
  - средства мгновенного обмена сообщениями – SIP, Skype, Telegram, Viber (с возможностью перехвата и архивирования вложенных файлов, текстовых и голосовых данных), Microsoft Lync (голосовые и текстовые сообщения), Slack (текстовые сообщения и файлы), AIM, ICQ, Miranda, Mail.Ru Агент, Google Hangouts, PSI, QIP Infium, WhatsApp, Yahoo! Messenger и др., в т.ч. использующие шифрование;
  - запись файлов на внешние накопители;
  - запись файлов на локальные сетевые ресурсы;
  - отправка файлов в облачные сервисы хранения информации (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск);
  - отправка файлов на печать на локальные и сетевые принтеры;
  - передача файлов в компьютерных сетях по протоколам FTP и FTPS;
- мониторинг событий разглашения конфиденциальной информации в разговорной речи путем контроля аудио потока с микрофона контролируемой рабочей станции в режиме реального времени;
- поддержка удаленного доступа к просмотру видеоизображения рабочего стола компьютера пользователя в режиме реального времени;
- мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов;
- сбор и хранение всех исходящих и входящих электронных сообщений, с возможностью полнотекстового поиска по архиву, в том числе и в присоединенных к письмам файлах;
- поиск информации и формирование политик безопасности по группам Active Directory;
- контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного

назначения);
- контроль эффективности использования рабочего времени и ресурсов персоналом компании путем снятия снимков экрана, сбора информации по времени работы/простоя ПК, используемым приложениям (в том числе WinRT (Metro) и виртуальные рабочие столы), а также статистического и событийного анализа перехваченной информации;
- контроль инцидентов безопасности и анализ присвоенных им показателей уровня риска;
- запрет запуска отдельных программных приложений;
- возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности);
- блокирование сетевого трафика отдельных процессов;
- возможность блокирования передачи исходящих сообщений по протоколам SMTP, HTTP и MAPI (в т.ч. с использованием шифрования), содержащих определенную информацию на основе контентного и атрибутивного анализа сообщений и вложенных данных.

2. Требования к техническим и функциональным характеристикам системы

Система должна поддерживать несколько схем перехвата трафика в контролируемой сети, а также их комбинации:

- централизованный перехват данных с сетевого коммутатора;
- перехват данных с рабочих станций пользователей;
- перехват электронной почты, переданной через почтовые сервера;
- перехват HTTP(S)-трафика, переданного через прокси-сервера.

2.1 Требования к реализации централизованного перехвата данных

Система должна обеспечивать:

- перехват данных, отправляемых по протоколам, не использующим шифрование (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M) ;
- фильтрация данных, отправляемых по протоколу HTTP;
- гибкая настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным MAC-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, процессам.

2.2 Требования к перехвату данных с рабочих станций

Система должна поддерживать установку независимых программных модулей контроля непосредственно на рабочие станции сети организации.
Модуль должен осуществлять перехват нешифрованного сетевого трафика, а также выполнять перехват SSL-трафика и данных, переданных по использующим шифрование протоколам.
Модуль должен фиксировать активность пользователя на контролируемой рабочей станции.
Контроль рабочих станций должен обеспечивать следующее:

- возможность как централизованной установки модулей - из единой консоли управления либо средствами групповых политик домена (с использованием MSI-пакета), так и установки вручную (с использованием отдельного EXE-инсталлятора модуля с графическим интерфейсом);
- централизованная настройка дистрибутива модуля для установки вручную;
- возможность перехвата данных, отправляемых по нешифрованным протоколам (FTP,

HTTP, IMAP, POP3, SMTP, MAPI, MMP (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M);

- возможность перехвата данных, отправляемых по шифрованным протоколам (с использованием SSL/TLS-шифрования), включая шифрованные протоколы передачи веб-трафика (HTTPS), корпоративной и внешней электронной почты (IMAPS, POP3S, SMTPS, MAPI over RPC over HTTP, MAPI over RPC, MAPI over HTTPS), мессенджеров, передачи файлов (FTPS), а также данных, переданных в облачных сервисах (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск) и приложениях Google Hangouts, Microsoft Lync, SIP, Skype, Telegram, Viber, WhatsApp;
- перехват данных, отправляемых по протоколам с использованием SSL/TLS-шифрования, осуществляется путем подмены цифрового сертификата. При этом должна поддерживаться возможность указания произвольного имени удостоверяющего центра в генерируемых системой сертификатах, а также возможность гибкой настройки подмены для использования различных сертификатов при перехвате различных SSL/TLS-соединений;
- возможность перехвата и автоматического дешифрования зашифрованных почтовых сообщений, содержащих цифровую подпись (включая вложенные в письма файлы), защищенных по стандарту S/MIME;
- возможность установки режима перехвата: только шифрованный либо нешифрованный трафик, весь трафик (шифрованный и нешифрованный);
- возможность создания политик фильтрации и блокирования трафика на основании атрибутов и содержимого перехватываемых данных;
- возможность фильтрации данных, отправляемых по протоколу HTTP/ HTTPS;
- возможность гибкой настройки исключений из перехвата по IP- адресам (отдельным и диапазону), протоколам, системным учетным записям пользователей, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, атрибутам процессов, вешним устройствам и локальным сетевым ресурсам;
- возможность блокирования передачи исходящих сообщений по протоколу SMTP(S) на основании заданных политик;
- возможность указания адресов электронной почты пользователей, активных в текущий момент, на компьютерах с установленными агентами.
- возможность блокирования передачи почтовых сообщений по протоколу MAPI (в том числе с использованием шифрования), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений и вложенных данных, на основании имени домена, DNS-имени и SID домена, имени компьютера и пользователя);
- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных);
- возможность блокирования посещения веб-ресурсов;
- блокирование поиска запрещенной информации в сети Интернет;
- возможность блокирования паразитного HTTP(S) трафика вредоносных и служебных программ;
- блокирование сетевого трафика процессов на основании их атрибутов и значения хеш-функций исполнительных файлов;
- настройка уведомлений пользователя рабочей станции о сработках блокировки устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика;
- настройка сообщений о блокировании устройств, запуска процессов, сетевого трафика процессов, HTTP- и MAPI-трафика;
- перехват web-коммуникаций пользователей в социальных сетях Facebook, Twitter,

ВКонтакте, Одноклассники. При этом должны поддерживаться: двунаправленный перехват сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев;

- перехват входящей и исходящей web-почты (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex) ;
- контроль данных, отправляемых на внешние накопители, принтеры, облачные хранилища и локальные сетевые ресурсы пользователей и терминальных серверов;
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к локальным сетевым ресурсам;
- аудит файловых операций, контроль передачи информации и блокирование доступа пользователей к облачным сервисам хранения информации при использовании веб-интерфейса и десктоп-приложений (Apple iCloud, Dropbox, Google Drive, OneDrive, Облако-О, Яндекс.Диск);
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к различным классам внешних накопителей информации с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер);
- аудит использования и контроль доступа для внешних устройств, подключенных к рабочей станции, и блокирование доступа с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- возможность сбора статистики по времени работы/простоя компьютера;
- контроль запуска приложений на компьютерах пользователей, а также длительность работы в каждом приложении (например, контроль использования нежелательного или запрещенного программного обеспечения в корпоративной сети);
- запрет запуска отдельных программных приложений на контролируемой рабочей станции на основании имени процесса, атрибутов исполнительного файла и значения хеш-функции;
- возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (нажатие клавиши Print Screen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения, блокировка каких-либо операций);
- перехват данных, помещаемых в буфер обмена с поддержкой исключения активности отдельных процессов из перехвата;
- контроль данных, вводимых пользователем с клавиатуры («кейлоггер») с возможностью исключения активности отдельных процессов из перехвата;
- прослушивание аудиопотока, поступающего с микрофонов, подключенных к рабочим станциям в режиме реального времени;
- возможность удаленного просмотра видеоизображения рабочего стола пользователя в режиме реального времени;
- автоматическая запись аудиопотока с микрофона и системных звуков, а также видеоизображения с рабочего стола и подключенной веб-камеры компьютера по расписанию;
- запись аудио- и видеопотоков вручную;
- автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя (по имени, по заданным атрибутам или значениям хеш-функций);
- настройка функциональных возможностей модулей применительно к различным объектам AD, отдельным компьютерам (группам компьютеров) и пользователям с указанным SID;
- выбор условий активации настроек модулей, например, наличие соединения с

сервером, наличие активного VPN-подключения, произвольное заданное условие;
- возможность защиты модуля на рабочей станции от несанкционированного удаления пользователем;
- возможность скрытия модуля на рабочей станции (включая скрытие процессов, служб, установочных файлов и папок);
- опциональное отображение иконки системы в панели задач контролируемой рабочей станции;
- сохранение функциональных возможностей модуля (автономный режим) в случае выноса рабочей станции за пределы корпоративной сети, сохранение всех данных перехвата. Автоматическое восстановление связи с серверной частью системы;
- возможность настройки автономного режима работы модуля;

Система должна отслеживать и отображать статистику по состоянию модулей контроля рабочих станций:
- поступление данных на сервер от каждого модуля,
- пользователей, контролируемых модулем;
- подключенные внешние устройства
- типы перехватываемых данных (протоколов).

Данные статистики должны быть доступны для экспорта.

2.3 Требования к перехвату HTTP-трафика, переданного через прокси-сервера

Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервера должен обеспечивать:
- возможность перехвата и фильтрации данных;
- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S) на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных.

2.4 Требования к перехвату электронной почты, переданной через почтовые сервера

Система должна поддерживать интеграцию с почтовыми серверами, развернутыми на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного обеспечения, обеспечивающего перехват всех почтовых сообщений, переданных и полученных с помощью почтовых серверов по протоколам POP3, SMTP, IMAP и MAPI.

2.5 Требования к функциям хранения и обработки данных

В части хранения и обработки данных система должна обеспечивать:
- хранение всех перехватываемых данных вне зависимости от настроек политик безопасности, настроенных средствами системы;
- возможность централизованного хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL, MySQL (на выбор);
- возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз. Поисковые операции выполняются по всем базам данных в группе. Для событий запуска ротации можно настроить выполнение скриптов (перед и/или после ротации);
- поддержка работы с базами данных, расположенных на разных серверах;
- возможность настройки правил записи данных в базы для регуляции, в какую базу или группу баз записывать информацию в зависимости от типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутной информации;
- возможность балансировки нагрузки по двум и более группам баз данных либо базам

данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно;
- возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;
- возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- возможность настройки расписания для репликации данных;
- возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;
- при переполнении очереди репликации сервер блокирует прием новых данных;
- отображение статистики репликации данных;
- возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;
- возможность сохранения файловых объектов большого размера на диск сервера, а не в базу. В базу данных при этом помещаются относительные пути к файлам;
- возможность настройки длительности хранения информации в базе данных в группе ротации, в том числе установки различной длительности хранения для различных типов данных (например, хранить почтовую переписку за последние 60 дней, а переписку через мессенджеры – за последние 30 дней);
- возможность очистки базы данных вручную через Консоль администратора;
- возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);
- возможность архивирования баз данных с последующим подключением к системе для осуществления поиска в них критичной информации;
- параллельную обработку данных, перехваченных по различным каналам передачи информации;
- настройку резервного хранилища модуля контроля рабочих станций в части ограничения размера и максимального периода хранения информации;
- настройку максимальной скорости передачи перехваченных данных с рабочих станций модулем контроля на сервер;
- асинхронный поиск по перехваченным данным (отображение результатов должно выполняться по мере их получения).
- возможность выборочного удаления пользователем перехваченной информации.

2.6 Требования к поддерживаемым форматам файлов

Система должна поддерживать обработку файлов следующих форматов:

- Adobe Acrobat (*.pdf)
- Ami Pro (*.sam)
- Ansi Text (*.txt)
- ASCII Text
- ASF (метаданные) (*.asf)
- CSV (Comma-separated values) (*.csv)
- DBF (*.dbf)
- DjVu
- DWG
- DXF
- EBCDIC
- EML files (электронные письма, сохраненные Outlook Express) (*.eml)

- Enhanced Metafile Format (*.emf)
- Eudora MBX файлы сообщений (*.mbx)
- Flash (*.swf)
- GZIP (*.gz)
- HTML (*.htm, *.html)
- JPEG (метаданные) (*.jpg)
- Lotus 1-2-3 (*.wk?, *.123)
- MBOX архивы электронных писем (включая Thunderbird) (*.mbx)
- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht)
- Microsoft Access (*.mdb)
- Microsoft Access 2007 (*.accdb)
- Microsoft Document Imaging (*.mdi)
- Microsoft Excel (*.xls)
- Microsoft Excel 2003 XML (*.xml)
- Microsoft Excel 2007 (*.xlsx)
- Microsoft Open XML Paper Specification (*.oxps)
- Microsoft Outlook (OST)
- Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx)
- Microsoft PowerPoint (*.ppt)
- Microsoft Rich Text Format (*.rtf)
- Microsoft Searchable Tiff (*.tiff)
- Microsoft Word 2003 XML (*.xml)
- Microsoft Word 2007 (*.docx)
- Microsoft Word for DOS (*.doc)
- Microsoft Word for Windows (*.doc)
- Microsoft Works (*.wks)
- MIME-сообщения
- MP3 (метаданные) (*.mp3)
- MSG files (электронные письма, сохраненные Outlook) (*.msg)
- Multimate Advantage II (*.dox)
- Multimate version 4 (*.doc)
- OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений)
- OST (внутренний формат Microsoft Outlook)
- Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)
- TAR (*.tar)
- TIFF (*.tif)
- TNEF (winmail.dat)
- Treepad HJT (*.hjt)
- Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)
- Windows Metafile Format (*.wmf)
- WMA видео (метаданные) (*.wma)
- WMV видео (метаданные) (*.wmv)
- WordPerfect (5.0 и выше) (*.wpd, *.wpf)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordStar 2000
- WordStar версий 1, 2, 3, 4, 5, 6 (*.ws)
- Write (*.wri)

- XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf)
- XML Paper Specification (*.xps)
- XSL
- XyWrite
- ZIP (*.zip)

Кроме того, система должна обеспечивать распознавание и анализ текстовой информации в файлах графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR). Должна поддерживаться возможность выбора между встроенным и сторонним средствами распознавания.

2.7 Требования к возможностям управления пользователями

В системе должно быть обеспечено следующее:

- создание внутренних профилей (карточек) пользователей, содержащих всю идентификационную информацию пользователей локальной сети;
- интеграция с Active Directory (возможность импорта всех идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя; возможность автоматического создания (удаления) профилей пользователей при добавлении (удалении) записей в (из) Active Directory, автоматическое создание карточек при обнаружении ранее не известной пользовательской информации, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями с возможностью настройки расписания синхронизации);
- возможность выборочной интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;
- возможность автоматической привязки идентификационных данных пользователя, отсутствующих в Active Directory (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя;
- возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей (например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании);
- возможность создания и редактирования пользовательских карточек;
- возможность отображения пользовательских карточек как в виде линейного списка, так и с разбивкой на группы и подгруппы на основании информации из Active Directory (с учетом Organizational Units), либо на основании задаваемых параметров в карточках пользователей (произвольная группировка по организациям/отделам);
- аутентификация пользователей, работающих с системой, на основании их учетных записей Windows и на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);
- возможность разграничения прав доступа к системе и ее компонентам для различных пользователей с назначением ролей (например, «системный администратор» - доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения» - доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности» - доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) на основе

аутентификации пользователей;
- политика сложности и срока действия паролей в режиме внутренней аутентификации;
- возможность отправки администратору уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения и т.д.);
- ведение журнала (лога) действий пользователей, работающих с системой.

3. Требования к перечню контролируемых каналов утечки

3.1 Требования к контролю электронной почты

Система должна обеспечивать контроль отправки информации посредством электронной почты, включая следующие возможности:

- перехват почтовых сообщений для нешифрованных и шифрованных (SSL) протоколов – IMAP, POP3, SMTP, MAPI плюс шифрованные аналоги;
- перехват почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME с автоматической расшифровкой содержимого письма;
- перехват почтовых сообщений путем интеграции с почтовыми серверами (на базе Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail и др.) по протоколам IMAP, POP3, SMTP (на выбор);
- перехват почтовых сообщений между Microsoft Outlook и Microsoft Exchange Server по протоколу MAPI (в том числе с использованием шифрования) путем интеграции с Microsoft Outlook;
- перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
- перехват и анализ файлов-вложений почтовых сообщений;
- автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- блокировка исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений;
- возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;
- возможность поиска по тексту и атрибутам почтовых сообщений и файлов, переданных по почте.

3.2 Требования к контролю IM-клиентов

Система должна обеспечивать контроль отправки информации посредством IM-клиентов, включая следующие возможности:

- перехват сообщений и файлов посредством зеркалирования трафика на сетевом коммутаторе (для протоколов MRA, OSCAR, XMPP, YMSG, не использующих шифрование);
- возможность перехвата текстовых сообщений модулями, установленными на рабочие станции пользователей (Google Hangouts, Microsoft Lync, MRA, OSCAR, SIP, Skype, Slack, Telegram, Viber, WhatsApp, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);
- возможность перехвата файлов, отправляемых с рабочих станций (Microsoft Lync, MRA, OSCAR, Skype, Slack, Telegram, Viber, XMPP, YMSG – как шифрованных (SSL), так и нешифрованных);

- возможность перехвата голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber и по протоколу SIP с сохранением разговоров;
- возможность распознавания (перевода в текстовый формат) голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber и SIP;
- возможность воспроизведения сохраненных разговоров Telegram, Skype, Viber, Microsoft Lync и SIP;
- возможность ограничения перехвата по отдельным учетным записям пользователей;
- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через IM-клиенты.

3.3 Требования к контролю HTTP-протокола

Система должна обеспечивать контроль отправки информации по HTTP-протоколу, включая:

- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола HTTP);
- возможность перехвата посредством интеграции с прокси-серверами по протоколу ICAP (для протоколов HTTP и HTTPS);
- возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов HTTP и HTTPS);
- возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;
- возможность создания и гибкой настройки фильтров для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователем;
- возможность настройки фильтрации перехвата данных по MIME-типам;
- перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;
- перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
- перехват сообщений, переданных в веб-клиентах ICQ и Skype ;
- перехват и анализ поисковых запросов пользователя;
- сохранение адресов всех страниц (URL), посещенных пользователем;
- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);
- возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов определенного содержания (HTTP и HTTPS);
- контроль браузер-активности (посещения веб-сайтов с помощью веб-браузера): фиксация переходов между страницами веб-сайтов и ведение комплексной статистики времени, проведенного на различных веб-ресурсах.

3.4 Требования к контролю FTP-протокола

Система должна обеспечивать контроль информации, передаваемой по протоколу FTP, включая возможности:

- перехвата файлов, загруженных или переданных по простому FTP-соединению, а также переданных по зашифрованному SSL-соединению;
- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола FTP);
- возможность перехвата данных модулями, установленными на рабочие станции пользователей (для протоколов FTP и FTPS);
- возможность настройки ограничения по размеру перехватываемых файлов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S).

3.5 Требования к контролю принтеров

Система должна обеспечивать контроль информации, отправляемой на печать, включая:

- возможность перехвата документов, отправляемых на сетевые и локальные принтеры (в том числе подключенные к COM-, LPT-портам);
- возможность перехвата печати в XPS-формат;
- возможность настройки исключений из перехвата по отдельным принтерам;
- возможность ограничения перехвата печати по количеству страниц и по размеру документа;
- возможность исключения процессов для модуля перехвата печати на принтерах.
- извлечение и анализ текста отправленных на печать документов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам отправленных на печать файлов;
- сохранение перехваченного текста (PDF и HTML-формат).

3.6 Требования к контролю подключенных устройств и внешних накопителей информации

Система должна обеспечивать контроль информации, отправляемой на внешние носители, включая:

- теневое копирование файлов, отправляемых на внешние накопители информации (съемные жесткие диски, карты памяти, съемные накопители, CD/DVD и флоппи-диски);
- возможность настройки исключений из теневого копирования по размеру и расширению файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- возможность настройки исключений из теневого копирования для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);
- контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя

производителя, идентификатор и название продукта, серийный номер, тип устройства);
- управление правами записи на внешние накопители информации с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;
- возможность контроля копирования информации на внешние накопители информации как в локальных, так и терминальных пользовательских сессиях;
- аудит событий копирования файлов на внешние накопители: должно фиксироваться имя файла, пользователь, дата, время и данные устройства;
- контроль доступа и аудит использования внешних устройств любого типа, подключаемых к рабочей станции, по набору параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам файлов, отправленных на внешние накопители информации.

3.7 Требования к контролю локальных сетевых ресурсов

Система должна обеспечивать контроль информации, отправляемой на локальные сетевые ресурсы, включая следующие возможности:

- теневое копирование файлов, отправляемых на сетевые ресурсы;
- возможность настройки исключений из теневого копирования по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- контроль доступа к сетевым ресурсам с возможностью запрета доступа для определенных пользователей;
- управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;
- возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;
- автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий копирования файлов на локальные сетевые ресурсы: фиксация имени файла, пользователь, дата, время и сетевой путь к ресурсу;
- возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов.

3.8 Требования к контролю облачных хранилищ (Apple iCloud, Dropbox, Google Drive, OneDrive, Диск-О, Яндекс.Диск)

Система должна обеспечивать контроль использования облачных хранилищ, в том числе:

- теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;
- возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;
- управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;
- автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий отправки файлов в облачные хранилища с фиксацией имени файла, имени пользователя, даты, времени и имени облачного сервиса хранения;
- возможность поиска по тексту и атрибутам отправленных файлов.

4. Требования к возможностям мониторинга действий пользователей на ПК

4.1 Требования к функции снятия скриншотов

Система должна выполнять сохранение снимков рабочего стола пользователей и обеспечивать:

- возможность снятия скриншотов с заданным интервалом с точностью до секунды;
- возможность снятия скриншотов при смене активного окна и смене вкладки браузера, запуске нового процесса;
- возможность снятия скриншотов при срабатывании правила блокировки;
- возможность снятия скриншотов при нажатии клавиши Print Screen;
- возможность настройки качества скриншотов (в т.ч. сохранения в черно-белом формате);
- возможность настройки размера скриншотов (в процентах от оригинала);
- возможность настройки формата скриншотов (JPEG, PNG);
- сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);
- возможность отключения захвата снимков при простое рабочей станции;
- возможность экспорта снимков экранов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;
- возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
- возможность сохранения скриншотов нескольких пользователей за выбранный интервал дат в виде набора графических файлов, web- документа либо объединенных в один PDF- или видео-файл;
- при просмотре скриншота отображается «watermark» с названием компьютера и именем пользователя.

4.2 Требования к функции сбора статистики по активности ПК

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих

станций и активности пользователя на рабочей станции:

- ведение статистики по времени работы и простоя (отсутствия действий пользователя) ПК с представлением собранной информации в виде графика;
- ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
- возможность настройки исключений отдельных процессов из мониторинга;
- возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в виде PDF-файла;
- возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу.

4.3 Требования к контролю буфера обмена

Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции:

- теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
- возможность ограничения максимального объема текста, перехватываемого из буфера обмена;
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, помещаемому пользователями в буфер обмена.

4.4 Требования к функциям кейлоггера

Система должна поддерживать:

- регистрацию нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных клавиш (Shift, Enter, Backspace и т.п.);
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, вводимому пользователями с клавиатуры.

4.5 Аудиомониторинг

Система должна обеспечивать возможность прослушивания звуковых потоков с рабочей станции, в том числе:

- подключение к микрофонам контролируемых рабочих станций с возможность прослушивания аудиопотока в режиме реального времени;
- прослушивание микрофонов нескольких пользователей одновременно;
- автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;

- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.6 Видеомониторинг

Система должна поддерживать:

- подключение к монитору компьютера пользователя и просмотра изображения рабочего стола в режиме реального времени;
- мониторинг рабочих столов нескольких пользователей одновременно;
- возможность вывода окна просмотра на отдельный экран;
- автоматическая запись видеоизображения рабочего стола и подключенной веб-камеры по расписанию;
- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

4.7 Требования к контролю файловых систем:

Контроль файловых систем должен позволять:

- формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;
- автоматическое сканирование дисков контролируемых компьютеров на предмет наличия определенных документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;
- возможность выбора компьютеров и пользователей, чьи файловые системы будут контролироваться;
- гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;
- возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций;
- возможность удаленного поиска документов в файловых системах контролируемых рабочих станций на основе атрибутов файлов и значения их хеш-функций.

5. Требования к методам анализа перехваченной информации и процедурам реагирования на инциденты безопасности

Система должна обеспечивать следующие функциональные возможности при работе с политиками безопасности:

- автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента); уведомление содержит общую информацию об инциденте (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента), а также ссылку на открытие соответствующего инцидента в пользовательской консоли;
- возможность указания групп Active Directory, к которым могут быть применены политики безопасности;
- возможность добавлять/исключать/редактировать категории и уровни риска инцидентов сервера безопасности для автоматического расчёта показателей уровней риска пользователей;
- возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в

сутки и т.д.);
- возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли (с индивидуальным выделением просмотренных/непросмотренных инцидентов для каждого офицера безопасности, работающего с системой);
- при просмотре информации об инциденте в клиентской консоли доступна следующая информация:
    - пользователь, допустивший нарушение;
    - дата и время инцидента;
    - показатель присвоенного уровня риска;
    - тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.);
    - содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности;
    - другая дополнительная информация.
- возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);
- возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые (непросмотренные) инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);
- возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);
- возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);
- возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;
- возможность экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);
- возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;
- ведение журнала (лога) действий офицера безопасности.

При анализе информации должны быть реализованы следующие возможности (аналитические возможности системы должны быть одинаковы для всех поддерживаемых языков анализируемой информации – включая анализ информации на английском, арабском, белорусском, испанском, казахском, китайском, корейском, немецком, русском и других языках):

Контентный анализ:

- поиск по словам и словосочетаниям с учетом морфологии (возможность отключения), расстояния между словами и порядка слов, транслитерации кириллических символов

латинскими, а также с возможностью нечеткого поиска (для поиска ключевых слов, в т.ч. написанных с ошибками и опечатками);
- поддержка регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;
- поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок/регулярных выражений в словарях, с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре);
- поиск документов с умышленно измененным расширением;
- поиск документов, защищенных паролем;
- цифровые отпечатки документов: возможность создания цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента совпадения);
- цифровые отпечатки баз данных: возможность настройки подключения системы к базе данных, содержащей конфиденциальную информацию, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой БД (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»). Создание и обновление цифровых отпечатков баз данных должно осуществляться без промежуточных действий (таких как выгрузка базы данных в файл-источник цифрового отпечатка). При внесении изменений в базу данных система должна автоматически обновлять соответствующие цифровые отпечатки.
- комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ».
- поиск данных по DNS-имени и SID компьютера, по имени и SID домена среди данных, перехваченных агентами.
- поиск информации по группам Active Directory.

Анализ по атрибутам

- анализ по атрибутам пользовательских документов, таким как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «размер» и пр.;
- анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных.
- анализ атрибутов процессов: имя исполняющего файла, полный путь к файлу, заголовок окна процесса.

Статистический анализ

- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем электронным письмам (например, «пользователь получил более 10 писем за час» или «пользователь отправил менее 20 писем за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем файлам (например, «пользователь получил более 10 файлов за час» или «пользователь отправил более 20 файлов за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по переписке пользователя в IM-клиентах (например,

«пользователь провел более 10 сессий переписки за день» или «пользователь отправил более 100 сообщений за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по голосовым переговорам в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по посещенным пользователем URL (например, «пользователь посетил более 100 URL за день», «пользователь посетил более 1000 URL за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по поисковым запросам пользователя (например, «пользователь отправил более 100 поисковых запросов в период с 13:00 до 15:00» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по данным, отправленным пользователем на печать (например, «пользователь распечатал более 10 документов за день» или «пользователь распечатал более 1000 страниц за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности/простоя ПК (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени работы пользователя с определенными приложениями (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

Событийный анализ

Возможность настройки автоматических уведомлений в следующих случаях:

- выявления факта запуска (завершения) пользователем определенного приложения;
- обнаружения пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);
- копирования файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;
- подключения и использования на контролируемых рабочих станциях устройств с определенными параметрами;
- блокирования пересылки данных по SMTP, HTTP, MAPI;
- посещение определенных web-ресурсов;
- обнаружения конфиденциальных файлов на компьютерных дисках пользователей;
- выявления факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения).

Анализ рисков

Возможность дополнить политики безопасности следующим функционалом:

- формировать модели поведения сотрудников и задавать им соответствующий уровень риска;
- информировать специалистов отдела безопасности об уровне риска и об инцидентах политик безопасности, которые вызвали изменения уровней риска;
- отслеживать изменения в поведении сотрудников в режиме реального времени.

Независимо от используемого типа анализа, система должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных данных (для выявления фактов нарушения вновь созданной политики безопасности в прошлом за весь период наблюдения).

6. Организация документов при проведении расследований

Система должна предусматривать специальный модуль для организации информации и документации для проведения расследований (типа «центр расследований»), который должен обеспечивать следующие возможности:

- в целях сбора доказательств по инцидентам безопасности -- создание документа (дела), который может включать в себя:
  - информацию об инциденте;
  - перечень вовлеченных лиц и их реквизиты;
  - перечень проводимых (проведенных) мероприятий по расследованию инцидента и их результаты;
  - выводы по результатам расследований;
  - материалы расследований – внутренние документы (результаты перехвата) системы;
  - реквизиты внутренних документов: тип данных, локальный пользователь, удаленный пользователь, дата перехвата, размер документа;
  - материалы расследований – внешние документы;
  - внешние документы, содержащие аналитические записки, рапорты и т.п.
- в целях комплексного аудита результатов перехвата обеспечивать функции:
  - просмотр содержания документов в расширенном виде напрямую из дела;
  - фильтрацию документов при просмотре в деле;
  - представление включенных в дело документов в режимах просмотра карточки, список;
  - возможность экспорта дела в форматы *.pdf, *.xps.
  - возможность распечатки дела на принтере.
- в целях контроля за внесением изменений в дело наличие журнала событий, включающего в себя информацию о всех вносимых правках:
  - имя пользователя, который совершил операцию в деле;
  - совершенное действие;
  - дату и время совершенного действия;
  - прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.
- в целях упрощения работы лиц, ведущих расследование обеспечивать:
  - ведение списка дел;
  - возможность сортировки дел в группы;
  - возможность создания групп и подгрупп с количество уровней иерархии не менее 20;
  - возможность переноса дел из группы в группу простым перетаскиванием «мышкой»;
  - возможность переноса подгрупп из группы в группу простым перетаскиванием «мышкой»;
  - возможность удаления дел и групп;
  - возможность исправления дел;
  - возможность просмотра: всех дел, только открытых дел, только закрытых дел;
  - возможность глубокой пользовательской настройки просмотра дел: всех дел за

определенный период; дел, открытых в определенный период; дел, закрытых в определенный период;
- возможность закрепления и открепления поля списка дел;
- возможность переноса поля списка дел к любой стороне окна программы.

Система также должна обеспечивать возможность удобного присоединения документов к делу в модуле типа «центр расследований» из других модулей системы: например, через контекстное меню.

8. Требования к отчетности

Все перехваченные данные должны представляться в форме отчетов следующих видов:
Отчет об активности пользователя

- Вкладка «Дневная активность» на временной сетке с шагом в 1 час должна содержать:
  - информацию о количестве отправленных и полученных пользователем писем;
  - информацию о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;
  - информацию о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах;
  - информацию о количестве посещенных URL и отправленных поисковых запросов;
  - информацию о количестве сделанных системой снимков экрана рабочего стола пользователя;
  - информацию о времени работы/простоя компьютера пользователя, детальную статистику активности приложений и данные о процентном соотношении времени работы в различных приложениях;
  - информацию о количестве документов, помещенных в буфер обмена;
  - информацию о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;
  - информацию о количестве символов, введенных пользователем с клавиатуры.

Вкладка должна быть интерактивная и динамическая, чтобы позволять осуществлять переход по ссылкам непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок. Должна быть обеспечена возможность экспорта дневной активности во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к перехваченным данным в веб-браузере, а также с возможностью сохранения выбора ассоциированных просмотрищиков для разных типов документов в расширенных настройках.

- Вкладка «Статистика по активности»

Система должна представлять данные, собранные по определенному пользователю за конкретный интервал времени, в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов). Графики по типам информации должны поддерживать интерактивность и динамичность, поддерживать возможность перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов.
Необходимо предусмотреть возможность сохранения статистики во внешний файл формата PDF и XPS.

- Вкладка «Взаимосвязи»

Система должна обладать возможностью графического отображения взаимосвязей пользователя (в

виде графа или таблицы) на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь обменивался какой-либо информацией в течение выбранного интервала времени.
Должна быть обеспечена поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.
Возможность просмотра взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.
Возможность выбора масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).
Возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.
Поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

Отчет по пользователям
Система должна реализовывать возможность построения сводного интерактивного отчета по определенному пользователю за все время наблюдения (или за выбранный интервал времени), включающего следующую информацию:

- статистика перехвата данных, в том числе
  - количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;
  - количество посещенных сайтов и поисковых запросов;
  - количество файлов, переданных/принятых по FTP;
  - количество распечатанных документов и страниц;
  - количество операций копирования в буфер обмена;
  - количество снятых скриншотов;
  - количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;
  - количество нажатых клавиш клавиатуры.
- информация об активности пользователя за компьютером, в том числе
  - общее время активной работы пользователя за ПК;
  - среднесуточное время активной работы пользователя за ПК;
  - общее время простоя ПК;
  - среднесуточное время простоя ПК;
  - общее время присутствия сотрудника на работе;
  - среднесуточное время присутствия сотрудника на работе;
  - среднее время начала работы;
  - среднее время окончания работы;
  - общее количество рабочих дней;
  - календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой);
  - гистограмма по времени активности/простоя компьютера пользователя за каждый день.
- информация об активности приложений на компьютере пользователя, в том числе
  - процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы);
  - полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них.
- информация о браузер-активности, в том числе
  - рейтинг посещенных веб-ресурсов;

- хронология активности в веб-браузере.
- информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.

Необходимо предусмотреть возможность пакетного сохранения отчетов для групп пользователей с предварительной настройкой единой формы отчета.

ТОП-отчет по пользователям

Система должна обеспечивать создание сводных интерактивных отчетов по всем контролируемым каналам передачи данных за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, наиболее активно использующих этот канал.

Система должна содержать возможность построения ТОП-отчета для сотрудников, входящих в группы пользователей системы либо в группы пользователей Active Directory.

Необходимо предусмотреть возможность построения сводных отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз.

При создании отчетов должна быть обеспечена возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов, то есть «Браузер активность: количество посещенных сайтов» и «Браузер активность: время проведенное на сайте».

тчет по политикам безопасности

Система должна обеспечивать возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, заданных в модуле Политики безопасности.

При этом система должна обеспечивать просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр итогового количества срабатываний по каждому правилу в отдельности и по всем существующим правилам безопасности.

Сводный отчет по пользователям

Система должна предусматривать возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей.

Также необходимо обеспечить просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики для выбранных статистических показателей.

10. Мониторинг работоспособности системы

Система должна поддерживать:

- ведение журнала событий серверных компонентов системы;
- просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;
- фильтрацию событий в журнале по рабочей станции, серверному компоненту, уровню, дате;
- выбор определенных рабочих станций для ведения мониторинга;
- автоматическое уведомление администратора системы о новых событиях серверных компонентов через консоль администратора и по почте;
- настройку правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

Систем должна фиксировать сведения о всех наиболее существенных событиях в работе серверных компонентов в журнале операционной системы рабочей станции, на которой они установлены.

11. Прочие требования

В процессе своего функционирования система не должна оказывать негативного влияния на функционирование прикладных ИС Заказчика.

Масштабируемость системы

В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы:

- возможность установки нескольких серверов перехвата данных для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;
- возможность установки нескольких серверов контроля агентов для контроля разных сегментов сети или разных групп компьютеров;
- возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;
- возможность установки нескольких серверов индексирования для оптимизации и распределения нагрузки на сервер и базу данных;
- возможность установки нескольких серверов обработки почты для работы с несколькими почтовыми серверами (MS Exchange, IBM Lotus Domino и др.).

Ориентация работы всех компонентов системы на многопоточность

Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах. С помощью добавочного модуля распознавания ABBYY должна существовать возможность распознавания одновременно нескольких PDF-документов.

Удобство администрирования

Система должна обеспечивать следующие функции, повышающие эффективность администрирования программы:

- Централизованное управление компонентами системы с использованием шифрования из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ).
- Возможность централизованного подключения и настройки хранилищ информации, а также создания резервной копии конфигурации всех серверных компонентов с поддержкой последующего восстановления настроек серверов через консоль администратора.
- Возможность автоматического переподключения к серверу при разрыве соединения с консолью пользователя.
- Возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности;
- Возможность отключения автоматического управления системным брандмауэром.
- Возможность при настройке профилей для агентов добавлять компьютер в профиль из схемы агентов, а также копировать/перемещать объекты между профилями.
- Автоматическая фиксация пользователей, которые проводят авторизацию или отклонении сервера-компонента на центральном сервере.

Политика лицензирования ПО

Система должна лицензироваться в соответствии с количеством контролируемых пользователей (500 лицензий для рабочих мест, включая 500 лицензий модуля распознавания изображений ABBYY, 600 лицензий на перехват сервером обработки корпоративной почты). При этом недопустимо использование жесткой привязки лицензии к конкретным рабочим станциям или пользователям. Количество приобретенных лицензий должно определять только количество одновременно контролируемых пользователей, при этом сам список контролируемых может быстро и гибко изменяться в случае необходимости (например, при наличии 100 пользователей в сети и только 50 лицензий – возможность контролировать выборочно сначала одних пользователей, затем других; при этом переназначение лицензионных слотов должно быть

возможно не реже 1 раза в сутки).

Система должна предусматривать возможность покомпонентной поставки, т.е. выбора типов контролируемых данных и отключения неиспользуемого функционала на уровне лицензии. Кроме того, лицензии должны быть бессрочны, в состав системы лицензирования должен быть включен 1 год техподдержки, а также внедрение и настройка Системы.

Покупатель:	Поставщик:
_____ /_____ /	_____ /_____/

Приложение № 4
к Документации

ОБОСНОВАНИЕ НАЧАЛЬНОЙ (МАКСИМАЛЬНОЙ) ЦЕНЫ ДОГОВОРА

Предмет договора: на предоставление неисключительных прав на использование программы для ЭВМ - Программный продукт «DLP система Falcon Gaze Secure Tower» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

1. Используемый метод определения начальной (максимальной) цены договора (далее – НМЦД) с обоснованием: метод сопоставимых рыночных цен (анализа рынка).
Заказчиком при определении НМЦД использовался метод сопоставимых рыночных цен (анализа рынка). Данный метод выбран в качестве приоритетного, применение иных методов определения НМЦД представляется нецелесообразным.

2. Для определения начальной (максимальной) цены договора были использованы следующие ценовые предложения:

- исх. 20017199 от 26.11.2020 г., ценовое предложение составляет – 10 105 000,00 рублей, НДС не облагается.
- исх. 6213/1 от 26.11.2020 г., ценовое предложение составляет – 9 221 800,00 рублей, НДС не облагается.
- исх. б/н от 27.11.2020 г., ценовое предложение составляет – 10 160 000,00 рублей, НДС не облагается.
- исх. б/н от 27.11.2020 г., ценовое предложение составляет – 9 121 800.00 рублей, НДС не облагается.

Начальная (максимальная) цена договора была определена по минимальному ценовому предложению.

Таким образом начальная (максимальная) цена договора составляет 9 121 800,00 (Девять миллионов сто двадцать одна тысяча восемьсот) рублей 00 копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.