EFSOL ES
ЭФФЕКТИВНЫЕ РЕШЕНИЯ

# Комплексный отчет по аудиту ИТ-безопасности структуры

**Заказчик:**

**Исполнитель:** **Группа компаний EFSOL**

## Оглавление

## 1. Физический контроль доступа в помещения, наблюдение за помещениями

| Текущее состояние | Оптимальная структура* | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| **Контроль физического доступа и перемещения сотрудников в помещениях Заказчика** | | | |
| Объект 1 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Наличие или отсутствие системы СКУД<br>Схема выдачи пропусков<br>Ограничение передвижение персонала<br>Наличие системы пропусков<br>Наличие регламентов<br>И т.д | <Описывается оптимальная структура><br>**Например:**<br>1.Доступ к зонам, где обрабатывается или хранится важная информация, должен управляться и быть ограничен только полномочными лицами; средства управления аутентификацией, например, карточка управления доступом плюс персональный идентификационный номер[PIN], должны использоваться, чтобы<br>разрешать и подтверждать любой доступ; контрольный журнал всего доступа должен содержаться в надежном месте;<br>2.Персоналу вспомогательных служб третьей стороны должен быть предоставлен<br>ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен<br>и должен постоянно контролироваться;<br>3.Права доступа в зоны безопасности должны регулярно анализироваться и обновляться, и отменяться, если необходимо;<br>4. Должны быть учены соответствующие нормы и стандарты по технике безопасности и охране труда;<br>5. Ключевые средства должны быть расположены так, чтобы избежать доступа к ним широкой публики;<br>6. Там, где это применимо, здания | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Отсутствие системы СКУД<br>2.Нет системы гибкого управления физическим доступом<br>3.Все внутренние отдельные помещения физически защищены обыкновенными замками<br>4..Отсутствие персональных идентификаторов[PIN]<br>5.Отсутствует анализ прав доступа в зоны безопасности | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Внедрить отдельные основной и резервный сервер для ПО СКУД<br>2.Закупить и установить контроллеры и электронные замки для каждого отдельного помещения<br>3.Подключить контроллеры дверей к центральной системе СКУД<br>4.Настроить систему СКУД согласно техническому заданию, с учетом разрешенных уровней доступа групп сотрудников и времени суток к зонам, где обрабатывается или хранится информация.<br>5.Зафиксировать группы доступа в регламенте ИТ-безопасности<br>6.Регламентировать период проверки прав доступа в зоны безопасности<br>7.Проводить согласно регламенту проверку прав доступа в зону безопасности |

| | | | |
|---|---|---|---|
| | должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;<br>7. Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике. | | |
| Объект 2 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Наличие или отсутствие системы СКУД<br>Схема выдачи пропусков<br>Ограничение передвижение персонала<br>Наличие системы пропусков<br>Наличие регламентов<br>И т.д | ---------- | <Описываются текущие проблемы на объекте<br>**Например:**<br>1.Отсутствие системы СКУД<br>2.Нет системы гибкого управления физическим доступом<br>3.Все внутренние отдельные помещения физически защищены обыкновенными замками<br>4..Отсутствие персональных идентификаторов[PIN]<br>5.Отсутствует анализ прав доступа в зоны безопасности<br>> | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Зафиксировать группы доступа в регламенте ИТ-безопасности<br>2.Регламентировать период проверки прав доступа в зоны безопасности<br>3.Проводить согласно регламенту проверку прав доступа в зону безопасности |
| **Возможность доступа в офис Заказчика посторонних лиц в ночное и нерабочее время** | | | |
| Объект 1 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Как перемещаются сотрудники<br>Как используют пропускную систему<br>Как охраняется территория<br>И т.д | <Описывается оптимальная структура><br>**Например:**<br>1. От всех служащих, подрядчиков и пользователей третьей стороны и от всех посетителей надо требовать носить некоторую форму видимого идентификационного документа, и они должны немедленно сообщать персоналу службы безопасности, если они сталкиваются с посетителями без сопровождающего и с кем-либо, кто не носит видимого идентификационного документа;<br>2. Персоналу вспомогательных служб | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Посетители не носят выданные пропуска на видимом месте<br>2. Система сигнализации периметра и помещений отсутствует. | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Необходимо административно закрепить обязательство видимых идентификационных документов сотрудников.<br>2. Необходимо обеспечить помещения с центрами обработки информации средствами сигнализации. |

| | | | |
|---|---|---|---|
| | третьей стороны должен быть предоставлен<br>ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен и должен постоянно контролироваться;<br>3.Ключевые средства должны быть расположены так, чтобы избежать доступа к<br>ним широкой публики;<br>4. Там, где это применимо, здания должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;<br>5. Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.<br>6. Фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;<br>7. Необходимо избегать безнадзорной работы в безопасных зонах;<br>8. Рекомендовано устанавливать средства сигнализационного оповещения и мониторинга доступа лиц в помещения. | | |
| Объект 2 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Как перемещаются сотрудники<br>Как используют пропускную систему<br>Как охраняется территория<br>И т.д | <Описывается оптимальная структура><br>**Например:**<br>1. От всех служащих, подрядчиков и пользователей третьей стороны и от всех посетителей надо требовать носить некоторую форму видимого идентификационного документа, и они должны немедленно сообщать | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Посетители не носят выданные пропуска на видимом месте<br>2. Система сигнализации периметра и помещений отсутствует. | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Необходимо административно закрепить обязательство видимых идентификационных документов сотрудников.<br>2. Необходимо обеспечить |

| | | | |
|---|---|---|---|
| | персоналу службы безопасности, если они сталкиваются с посетителями без сопровождающего и с кем-либо, кто не носит видимого идентификационного документа;<br>2. Персоналу вспомогательных служб третьей стороны должен быть предоставлен<br>ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен<br>и должен постоянно контролироваться;<br>3.Ключевые средства должны быть расположены так, чтобы избежать доступа к<br>ним широкой публики;<br>4. Там, где это применимо, здания должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;<br>5. Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.<br>6. Фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;<br>7. Необходимо избегать безнадзорной работы в безопасных зонах;<br>8. Рекомендовано устанавливать средства сигнализационного оповещения и мониторинга доступа лиц в помещения. | | помещения с центрами обработки информации средствами сигнализации. |
| **Возможность доступа в офис Заказчика посторонних лиц с преступными целями в рабочее время** | | | |
| Объект 1 | | | |
| <Описывается текущее состояние на объекте> | <Описывается оптимальная структура> | <Описываются текущие проблемы на | <Описываются текущие |

| | | | |
|---|---|---|---|
| **Например:**<br>Блокируется ли вход на КПП<br>Какие действия просходят при попытках проникнуть на территорию<br>Как ведут себя сотрудники при появлении контролирующих гос. Органов<br>и т.д | **Например:**<br>1. От всех служащих, подрядчиков и пользователей третьей стороны и от всех посетителей надо требовать носить некоторую форму видимого идентификационного документа, и они должны немедленно сообщать персоналу службы безопасности, если они сталкиваются с посетителями без сопровождающего и с кем-либо, кто не носит видимого идентификационного документа;<br>2. Персоналу вспомогательных служб третьей стороны должен быть предоставлен<br>ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен<br>и должен постоянно контролироваться;<br>3.Ключевые средства должны быть расположены так, чтобы избежать доступа к<br>ним широкой публики;<br>4. Там, где это применимо, здания должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;<br>5. Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.<br>6. Фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;<br>7. Необходимо избегать безнадзорной работы в безопасных зонах. | объекте><br>**Например:**<br>Посетители не носят выданные пропуска на видимом месте | проблемы на объекте><br>**Например:**<br>Необходимо административно закрепить обязательство видимых идентификационных документов сотрудников.<br>Рекомендуется подключение охранных тревожных кнопок для оповещения о вторжении и оперативного вызова соответствующих служб. |

| | | | |
|---|---|---|---|
| Объект 2 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Блокируется ли вход на КПП<br>Какие действия просходят при попытках проникнуть на территорию<br>Как ведут себя сотрудники при появлении контролирующих гос. Органов<br>и т.д | ---------- | <Описываются текущие проблемы на объекте><br>**Например:**<br>Замечания отсутствуют | <Описываются текущие проблемы на объекте><br>**Например:**<br>Структура соответствует стандартам |
| | | | |
| **Система отчетности и оповещений о доступе и перемещении в офисе Заказчика, визуального контроля над сотрудниками и посетителями** | | | |
| Объект 1 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Наличие системы видеонаблюдения<br>Описание системы видеонаблюдения<br>Наличие системы СКУД<br>И т.д | <Описывается оптимальная структура><br>**Например:**<br>Обязательные для всех СОТ (система охранная телевизионная) устройства:<br>• телевизионная камера;<br>• видеомонитор;<br>• источник электропитания, в том числе, резервного электропитания;<br>• соединительные линии.<br>Обязательными для всех систем являются следующие функциональные характеристики:<br>• телевизионный анализ изображений с помощью одной или нескольких ТК;<br>• синтез телевизионных изображений, полученных от всех ТК;<br>• сопровождение цели;<br>• приоритетное отображение тревожных событий;<br>• сигнализация о несанкционированных действиях.<br>Системы должны обеспечивать возможность круглосуточной работы;<br>Рекомендован отдельный регистрационный аппарат для хранения и архивации видеоматериала. | <Описываются текущие проблемы на объекте><br>**Например:**<br>Срок хранения резервных копий с видеокамер ограничен<br>Отсутсвие камер видеонаблюдения в серверных помещениях | <Описываются текущие проблемы на объекте><br>**Например:**<br>В случае отсутствия камер наблюдений в серверной необходимо их установить |
| Объект 2 | | | |
| <Описывается текущее состояние на объекте><br>**Например:** | ---------- | <Описываются текущие проблемы на объекте> | <Описываются текущие проблемы на объекте> |

| | | | |
|---|---|---|---|
| Наличие системы видеонаблюдения<br>Описание системы видеонаблюдения<br>Наличие системы СКУД<br>И т.д | | **Например:**<br>Срок хранения резервных копий с видеокамер ограничен<br>Отсутсвие камер видеонаблюдения в серверных помещениях | **Например:**<br>В случае отсутствия камер наблюдений в серверной необходимо их установить |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ГОСТ 26342-84 (2001) «Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры»
- ГОСТ Р 50658-94 (2001) «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений»
- ГОСТ Р 50659-94 (2001) «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 5. Радиоволновые доплеровские извещатели для закрытых помещений»
- ГОСТ Р 50775-95 «Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения»
- ГОСТ Р 50776-95 «Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию»
- ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»
- ГОСТ Р 51558-2000 «Системы охранные телевизионные. Общие технические требования. Методы испытаний»
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .
- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

## 2. Аппаратное обеспечение информационной системы

| Текущее состояние | Оптимальная структура | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| **Защищенность помещения, возможность получения доступа и наличие специальных защитных монтажных изделий, в которых физически расположена серверная и коммутационная структура** | | | |
| Объект 1 комната 1 | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Дверца шкафа открыта кабели неупорядоченные<br>находится близко к проходу. | <Описывается оптимальная структура><br>**Например:**<br>1. Силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;<br>2. Сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны;<br>3. силовые кабели должен быть отделены от кабелей дальней связи для того, чтобы предотвратить помехи;<br>4. легко различимые маркировки кабелей и оборудования должны использоваться для того, чтобы минимизировать ошибки из-за неправильного обращения, такие как случайная коммутация неправильных сетевых кабелей;<br>5. для того, чтобы снизить возможность ошибок, должен использоваться документированный список коммутаций;<br>6. для важных или критических систем, дополнительные средства управления, которые надо рассмотреть, включают в себя следующее:<br>а) установка бронированного кабельного канала и запертых комнат или блоков в контрольных точках и точках прерывания;<br>б) использование альтернативных маршрутизаций и/или средств передачи данных, обеспечивающих подходящую защиту;<br>в) использование оптоволоконного кабеля;<br>г) использование электромагнитного экранирования для защиты кабеля;<br>д) инициация технических зачисток и физического | <Описываются текущие проблемы на объекте><br>**Например:**<br>Есть беспрепятственный доступ к коммутационному оборудованию; | <Описываются текущие проблемы на объекте><br>**Например:**<br>Необходимо закрыть дверь коммутационного шкафа на замок<br>. |

| | | | |
|---|---|---|---|
| | контроля на предмет наличия неразрешенных устройств, присоединенных к кабелю;<br>е) контролируемый доступ к коммутационным панелям и кабельным комнатам;<br>7.Средства обработки информации, обращающиеся с важными данными, должны<br>располагаться так и иметь такой угол видимости, чтобы снизить риск того, что<br>информацию увидят посторонние лица в ходе их использования, а средства<br>хранения должны охраняться для того, чтобы избежать неразрешенного доступа;<br>8.Должны быть созданы средства управления для того, чтобы минимизировать риск возможных физических угроз, например, кража, пожар, взрывоопасные вещества, дым, вода(или сбой в подаче воды), пыль, вибрации, химические воздействия, помехи электроснабжению, помехи связи, электромагнитное излучение и вандализм;<br>9.Должны быть определены руководящие указания по употреблению пищи, напитков и курению вблизи средств обработки информации;<br>10. Внешние условия, такие как температура и влажность, должны постоянно контролироваться на наличие условий, которые могли бы негативно повлиять на работу средств обработки информации;<br>11. Защита от молнии должна быть применена ко всем зданиям, и молниезащитные фильтры должны быть установлены на все входящие линии электропередач и линии связи;<br>12. Оборудование, обрабатывающее важную информацию, должно быть защищено для того, чтобы минимизировать риски утечки информации по каналам побочных излучений. | | |
| Помещение 2 кабинет 2 | | | |
| Наличие инвентаризационной системы учета и привязки рабочих станций к конкретным пользователям системы | | | |
| Помещение 1 кабинет 2 | | | |
| <Описывается текущее состояние на объекте><br>**Например:** | <Описывается оптимальная структура><br>**Например:**<br>1.В организации должна присутствовать | <Описываются текущие проблемы на объекте><br>**Например:** | <Описываются текущие проблемы на объекте><br>**Например:** |

| | | | |
|---|---|---|---|
| Какое ПО используется для инвентаризации<br>Как проходит инвентаризация<br>И т.д | инвентаризационная система и система учета материальных ценностей ИТ-структуры.<br>2. Система должна обеспечивать следующие требования:<br>• Каталогизация;<br>• Описательная часть и характеристики;<br>• Автоматический сбор и пополнение информации;<br>• Документы движения и расхода ценностей;<br>• Разграничение доступа в систему. | материальные ценности ИТ-структуры<br>Текущая система не обеспечивает требуемый уровень автоматизации ведения учета ИТ. | Необходимо иметь одну общую систему или комбинацию между разными системами инвентаризации с одним общим интегратором (выгрузка/загрузка или обмен данными). |
| Возможность получения доступа и вирусного заражения пользовательских рабочих станций через внешние устройства - съемные носители информации, внешние накопители, floppy и CD накопители | | | |
| Все здания | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Практически на всех рабочих станциях разрешен доступ к съемным носителям. | <Описывается оптимальная структура><br>**Например:**<br>1. Накопители со сменным носителем должны быть разрешены только в том случае, если для этого есть производственная необходимость.**<br>2.Чтобы исключить злонамеренные действия в отношении конфиденциальной информации, требуется бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, особенно в нерабочее время;<br>3.Носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или шкафу), особенно когда помещение пустует; | <Описываются текущие проблемы на объекте><br>**Например:**<br>Разрешен доступ к съемным носителям. Доступ к съемным носителям может привести к утечке информации или к заражению рабочих станций вирусом или | <Описываются текущие проблемы на объекте><br>**Например:**<br>Физическим или программным способом отключить использование сменных носителей сотрудникам, для которых использование данных носителей не является обязательным, согласно должностных инструкций. |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .

- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

** Сменные носители включают в себя ленты, флэш-диски, съемные жесткие диски, CD-, DVD-диски и печатные носители информации.

## 3. Сетевое обеспечение информационной системы

| Текущее состояние | Оптимальная структура* | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| Наличие общедоступных участков кабельной системы с возможностью неконтролируемого подключения специальных устройств | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br><br>Комната 1- не закрыт сетевой шкаф.<br>Кабеля находятся в доступном месте<br>Не защищены кабел ьканалами<br>Розетки отсутствуют | <Описывается оптимальная структура><br>**Например:**<br><br>1. Силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;<br>2. Сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны;<br>3. Силовые кабели должен быть отделены от кабелей дальней связи для того, чтобы предотвратить помехи;<br>4. Легко различимые маркировки кабелей и оборудования должны использоваться для того, чтобы минимизировать ошибки из-за неправильного обращения, такие как случайная коммутация неправильных сетевых кабелей;<br>5.Для того, чтобы снизить возможность ошибок, должен использоваться документированный список коммутаций;<br>6. Для важных или критических систем, дополнительные средства управления, которые надо рассмотреть, включают в себя следующее:<br>а) установка бронированного кабельного канала и запертых комнат или блоков в контрольных точках и точках прерывания;<br>б) использование альтернативных маршрутизаций и/или средств передачи данных, обеспечивающих подходящую защиту;<br>в) использование оптоволоконного кабеля;<br>г) использование электромагнитного экранирования для защиты кабеля;<br>д) инициация технических зачисток и | <Описываются текущие проблемы на объекте><br>**Например:**<br><br>Не все сетевые кабеля защищены (не уложены в короба или кабель каналы)<br>Некоторые силовые кабеля не отделены от кабелей дальней связи | <Описываются текущие проблемы на объекте><br>**Например:**<br><br>Для важных и критических систем необходимо использовать:<br>-Альтернативные маршрутизаторы или средства передачи данных<br>-Проводить периодические проверки на наличие неразрешенных устройств подсоединённых к кабелю. |

| | | | |
|---|---|---|---|
| | физического контроля на предмет наличия неразрешенных устройств, присоединенных к кабелю;<br>е) контролируемый доступ к коммутационным панелям и кабельным комнатам;<br>7.Средства обработки информации, обращающиеся с важными данными, должны располагаться так и иметь такой угол видимости, чтобы снизить риск того, что информацию увидят посторонние лица в ходе их использования, а средства хранения должны охраняться для того, чтобы избежать неразрешенного доступа;<br>8.Должны быть созданы средства управления для того, чтобы минимизировать риск возможных физических угроз, например, кража, пожар, взрывоопасные вещества, дым, вода(или сбой в подаче воды), пыль, вибрации, химические воздействия, помехи электроснабжению, помехи связи, электромагнитное излучение и вандализм;<br>9.Должны быть определены руководящие указания по употреблению пищи, напитков и курению вблизи средств обработки информации;<br>10. Внешние условия, такие как температура и влажность, должны постоянно контролироваться на наличие условий, которые могли бы негативно повлиять на работу средств обработки информации;<br>11. Защита от молнии должна быть применена ко всем зданиям, и молниезащитные фильтры должны быть установлены на все входящие линии электропередач и линии связи;<br>12. Оборудование, обрабатывающее важную информацию, должно быть защищено для того, чтобы минимизировать риски утечки информации по каналам побочных излучений. | | |
| Возможность подключения и взлома посторонним лицом либо гостем сети Заказчика через физические и беспроводные сетевые соединения | | | |
| <Описывается текущее состояние на | <Описывается оптимальная структура> | <Описываются текущие проблемы на | <Описываются текущие проблемы на |

| | | | |
|---|---|---|---|
| объекте><br>**Например:**<br>На сетевом оборудованиии существует привязка по портам для пользователей | **Например:**<br><br>1. Силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;<br>2. Сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны;<br>3. силовые кабели должен быть отделены от кабелей дальней связи для того, чтобы предотвратить помехи;<br>4. Легко различимые маркировки кабелей и оборудования должны использоваться для того, чтобы минимизировать ошибки из-за неправильного обращения, такие как случайная коммутация неправильных сетевых кабелей;<br>5. Для того, чтобы снизить возможность ошибок, должен использоваться документированный список коммутаций;<br>избежать неразрешенного доступа; | объекте><br>**Например:**<br><br>Уязвимости описаны в п.5 – Экспресс-тесты | объекте><br>**Например:**<br>Замечания отсутствуют |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .
- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

## 4. Системное программное обеспечение

| Текущее состояние | Оптимальная структура* | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| Состояние лицензионности программного обеспечения (серверного и пользовательского) | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>В компании используется лицензионное а также бесплатное ПО. | <Описывается оптимальная структура><br>**Например:**<br>1.Все программное обеспечение в компании должно быть лицензионное<br>2.Все программное обеспечение должно быть описано | <Описываются текущие проблемы на объекте><br>**Например:**<br>Также у некоторых пользователей присутствует другое нелицензионное ПО<br>(п.14 – Пользовательская структура) | <Описываются текущие проблемы на объекте><br>**Например:**<br>Необходимо удалить все нелицензионное программное обеспечения рабочих станций пользователей |
| Показатель уровня защиты внутренней сети от атак извне через открытые порты и уязвимости интернет-шлюзов | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Из сети интернет доступны только почтовые сервера | <Описывается оптимальная структура><br>**Например:**<br>Из внешней сети должны быть открыты только те порты которые необходимы для корректной работы пользователей | <Описываются текущие проблемы на объекте><br>**Например:**<br>Замечания отсутствуют | <Описываются текущие проблемы на объекте><br>**Например:**<br>Отсутствуют |
| Наличие, актуальность и оптимальность функционирования антивирусной системы, актуальности антивирусных баз, сигнатур, настроек агентов у пользователей | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>В сети используется корпоративные антивирусное ПО Kaspersky. | <Описывается оптимальная структура><br>**Например:**<br>1.Наличисе централизованной антивирусной системы<br>2.Наличие централизованной системы управления и обновления антивирусным ПО<br>3.Наличие политик очистки и удаления вредоносных программ | <Описываются текущие проблемы на объекте><br>**Например:**<br>У некоторых пользователей не установлены последние обновления, антивирус находится в режиме предустановки<br>(п.14 – Пользовательская структура) | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Необходимо устранить причины по которым антивирусное по  не обновляется<br>2.Необходимо устранить причины по которым на некоторых рабочих станциях антивирусное по не запущено и не работает в активном режиме. |
| Результат проверки актуальности системных обновлений Microsoft для обеспечения закрытия критических уязвимостей и "дыр" ПО | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Используется сервер wsus который позволяет проводить в сети необходимые обновления ПО и ОС. Обновляются каждый день. | <Описывается оптимальная структура><br>**Например:**<br>В компании должна действовать политика обновлений ОС | <Описываются текущие проблемы на объекте><br>**Например:**<br>На некоторых рабочих станциях не установлены последние обновления (п.14 – Пользовательская структура) | <Описываются текущие проблемы на объекте><br>**Например:**<br>Необходимо устранить причины по которым рабочие станции не обновляются |
| Соответствие паролей на сервера и рабочие станции международным критериям криптозащиты | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Пароли на сервера и рабочие станции соответствуют международным | Пароль должен быть не менее 6 символов, содержать цифры а также буквы верхнего и нижнего регистров | <Описываются текущие проблемы на объекте><br>**Например:**<br>Замечания отсутствуют | <Описываются текущие проблемы на объекте><br>**Например:**<br>Отсутствуют |

| | | | |
|---|---|---|---|
| критериям криптозащиты | | | |
| Результат проверки ограниченности доступа и защищенности файлов, содержащих резервные копии корпоративных данных | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Доступ к резервным копиями ограничен. Получить доступ под тестовой учетной записью или записью гостя не удалось | <Описывается оптимальная структура><br>**Например:**<br>1.Резервные копии должны быть защищены паролем<br>2.Резервные копии должны хранится в надежном месте<br>3.Резервные копии должны постоянно проверятся<br>4.Резервные копии должны находится на достаточном удалении от источника копирования | <Описываются текущие проблемы на объекте><br>**Например:**<br>Резервные копии находятся в том же помещении что и сервера | <Описываются текущие проблемы на объекте><br>**Например:**<br>Необходимо настроить резервное копирование таким образом чтобы резервные копии находились на достаточном отдалении от основного места хранения информации. Это позволит сохранить доступность информации даже при стихийном бедствии, пожаре и т.п |
| | | | |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .
- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

## 5. Проведение экспресс-тестов

- Сканирование локальной сети на открытые ресурсы, поиск общедоступных ресурсов;
- Подключение к серверным и периферийным устройствам по сети, возможность вывода их из строя;
- Проведение сканирования внешних портов, фиксирование точек успешных атак через найденные уязвимости;
- Проверка файлов резервных копий, попытка найти, увидеть, открыть, скачать, удалить их под правами пользователя;
- Подключение к сети, вычисление серверных ресурсов, попробовать выложить документы на внешний ресурс.

| | |
|---|---|
| Высокое | 7.0-10.0 единиц по шкале CVSS* |
| Среднее | 4.0-6.9 единиц по шкале CVSS* |
| Низкое | 0-3.9 единиц по шкале CVSS* |

* CVSS - Общая система оценки уязвимостей

| Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|
| ip 192.168.3.3 | |
| Не доверенный SSL сертификат<br>**CVSS Base Score: 6.4**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:Nf**<br><br>Серверный X.509 сертификат не имеет подписи из известных публичных центров сертификации | Покупка или генерация соответствующего сертификата для данного сервера |
| Удаленная служба поддерживает средний уровень шифрования SSL<br><br>**CVSS Base Score: 4.3**<br>**CVSS Vector Score: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N**<br><br>Удаленный хост поддерживает SSL шифрование среднего уровня (длина ключа не менее 56 бит и не более 112 бит). | Перенастройка соответствующего приложения, если это возможно, на использование более стойкого шифрования |
| Удаленная служба шифрует трафик, используя протокол с известными уязвимостями (SSL версия 2)<br><br>Ссылки по данной уязвимости:<br>http://www.schneier.com/paper-ssl.pdf<br>http://support.microsoft.com/kb/187498<br>http://www.linux4beginners.info/node/disable-sslv2<br><br>**CVSS Base Score: 5.0**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N**<br><br>**cve:CVE-2005-2969:**<br>**http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2969** | Отключить использование протокола SSLv2 и включить поддержку SSLv3 и TLSv1 |

| | |
|---|---|
| Удаленная служба принимает подключения с помощью SSLv2 который имеет несколько криптографических уязвимостей и не рекомендуется для использования. Злоумышленник может использовать эти уязвимости для проведения атак и расшифровки связи между атакуемым сервисом и клиентами. | |
| SSL сертификат использует неправильное имя хоста (IT). Выявленные имена хостов<br>pop.avia-group.ru<br>smtp.avia-group.ru<br><br>**CVSS Base Score: 5.0**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N**<br><br>CommonName (CN) из SSL сертификата для этого сервиса использует другое имя хоста. | Покупка или генерация соответствующего сертификата для данного сервера |
| Служба SMTP имеет STARTTLS уязвимость отправки команд в открытом виде<br><br>Удаленный SMTP сервер позволяет внедрить команды в открытом виде но начала фазы TLS<br><br>Ссылки по данной уязвимости:<br>http://tools.ietf.org/html/rfc2487<br>http://www.securityfocus.com/archive/1/516901/30/0/threaded<br><br>**CVSS Base Score: 4.0**<br>**CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N**<br>**CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C**<br>**CVSS Temporal Score: 3.3**<br><br>**cve:CVE-2011-2165,CVE-2011-1506,CVE-2011-1432,CVE-2011-1431,CVE-2011-1430,CVE-2011-0411**<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2969<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1506<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1432<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1431<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1430<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0411 | Связаться с поставщикам для обновления службы или сервиса, если обновление доступно. |
| Удаленная служба поддерживает использование шифра RC4.<br><br>Удаленный хост поддерживает использование RC4 в одном или нескольких наборах шифров. Шифр RC4 имеет недостатки в генерации псевдослучайного потока байтов<br><br>Если открытый текст зашифрован неоднократно (например HTTP cookies) и атакующий может получит много шифртекстов, есть вероятность получить данные в открытом виде<br><br>Ссылки по данной уязвимости: | Перенастройка службы или приложения, если это возможно, на использование другого шифра |

| | |
|---|---|
| http://www.nessus.org/u?217a3666<br>http://cr.yp.to/talks/2013.03.12/slides.pdf<br>http://www.isg.rhul.ac.uk/tls/<br><br>CVSS Base Score: 2.6<br>CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N<br>CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:C<br>CVSS Temporal Score: 2.2<br><br>cve:CVE-2013-2566<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566 | |
| 192.14.3.8 | |
| PHP 5.3 < 5.3.27 имеет множественные уязвимости<br><br>Удаленный Web сервер использует версию PHP которая имеет множественные уязвимости<br><br>Дополнительные ссылки по данной уязвимости:<br>http://bugs.php.net/64949<br>http://bugs.php.net/65236<br>http://www.php.net/ChangeLog-5.php#5.3.27<br><br>**CVSS Base Score: 9.3**<br>**CVSS Vector Score: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C**<br>**CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C**<br>**CVSS Temporal Score: 6.9**<br><br>cve:CVE-2013-4113<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4113 | Обновить версию PHP до версии 5.3.27 или выше |
| Apache HTTP Server может быть подвержен DoS атакам<br><br>Версия Apache HTTP работающая на удаленном хосте может быть подвержена атакам нацеленным на уязвимость отказа в обслуживании. Проведя серию атак злоумышленник может вызвать отказ в обслуживании направленный на конечность ресурсов RAM и CPU<br><br>Дополнительные сведения по данной уязвимости:<br>http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html<br>http://www.gossamer-threads.com/lists/apache/dev/401638<br>http://www.nessus.org/u?404627ec<br>http://httpd.apache.org/security/CVE-2011-3192.txt<br>http://www.nessus.org/u?1538124a | Обновить Apache httpd до версии 2.2.21 или выше |

| | |
|---|---|
| http://www-01.ibm.com/support/docview.wss?uid=swg24030863<br><br>**CVSS Base Score: 7.8**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C**<br>**CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C**<br>**CVSS Temporal Score: 6.4**<br><br>cve:CVE-2011-3192:<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192 | |
| Прокси Web сервер XSS<br><br>Удаленный прокси-сервер подвержен XSS атакам. Прокси сервер не позволяет правильно сканировать строки запроса вредоносных JavaScript.<br><br>**CVSS Base Score: 4.3**<br>**CVSS Vector Score: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N**<br>**CVSS Temporal Vector: CVSS2#E:H/RL:U/RC:ND**<br>**CVSS Temporal Score: 4.3**<br><br>cve:CVE-2003-0292<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0292 | Связаться с поставщиком для получения заплатки или обновления |
| Apache 2.2 < 2.2.25 имеет множественные уязвимости<br><br>Удаленный Web-сервер может быть подвержен множественным крос-сайтовым уязвимостям<br><br>Дополнительные сведения по данной уязвимости:<br>http://www.apache.org/dist/httpd/CHANGES_2.2.25<br>http://httpd.apache.org/security/vulnerabilities_22.html<br>http://www.nessus.org/u?f050c342<br><br>**CVSS Base Score: 5.1**<br>**CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P**<br>**CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C**<br>**CVSS Temporal Score: 4.2**<br><br>**cve:CVE-2013-1862CVE-2013-1896**<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896 | Обновить Apache httpd 2.2.25 или выше. |
| Методы HTTP TRACE / TRACK разрешены | Отключить данные методы |

| | |
|---|---|
| Удаленный сервер поддерживает методы TRACE  и/или TRACK. Эти методы используются для отладки подключения к Web-серверу.<br><br>Дополнительные сведения по данной уязвимости:<br>http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf<br>http://www.apacheweek.com/issues/03-01-24<br>http://download.oracle.com/sunalerts/1000718.1.html<br><br>**CVSS Base Score: 4.3**<br>**CVSS Vector Score: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N**<br>**CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:C**<br>**CVSS Temporal Score: 3.9** | |
| 192.14.3.5 | |
| Xerox полные права на конфигурацию.<br><br>Изменение параметров данного устройство возможно без авторизационных данных.<br><br>**CVSS Base Score: 4.4**<br>**CVSS Vector Score: AV:L/AC:M/Au:N/C:P/I:P/A:P** | • Установить режим Администратора<br>• Установить логин и пароль |
| 192.14.3.3 | |
| **Не доверенный SSL сертификат**<br><br>Серверный X.509  сертификат не имеет подписи из известных публичных центров сертификации<br><br>**CVSS Base Score: 6.4**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N** | Покупка или генерация соответствующего сертификата для данного сервера |
| **Удаленный DNS сервер может быть подвержен cache snooping атакам.**<br><br>Удаленный сервер DNS отвечает на запросы сторонних доменов не имеющих установленный бит рекурсии.<br><br>Если к серверу нет доступа из сети интернет, атака возможна только на уровне локальной сети<br><br>Дополнительные данные:<br>http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf<br><br>**CVSS Base Score: 5.0**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N** | Свяжитесь с разработчиками службы DNS для решения проблемы |

| | |
|---|---|
| **Уровень шифрования Терминального сервера средний или низкий**<br><br>Удаленный хост использует средний уровень криптографии.<br><br>**CVSS Base Score: 4.3**<br>**CVSS Vector Score: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N** | Изменить уровень шифрования RDP на Высокий или FIPS-140 |
| Удаленная служба шифрует трафик, используя протокол с известными уязвимостями (SSL версия 2)<br><br>Ссылки по данной уязвимости:<br>http://www.schneier.com/paper-ssl.pdf<br>http://support.microsoft.com/kb/187498<br>http://www.linux4beginners.info/node/disable-sslv2<br><br>**CVSS Base Score: 5.0**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N**<br><br>**cve:CVE-2005-2969:**<br>**http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2969**<br><br>Удаленная служба принимает подключения с помощью SSLv2 который имеет несколько криптографических уязвимостей и не рекомендуется для использования. Злоумышленник может использовать эти уязвимости для проведения атак и расшифровки связи между атакуемым сервисом и клиентами. | Отключить использование протокола SSLv2 и включить поддержку SSLv3 и TLSv1 |
| **Самоподписанный сертификат SSL (порты 3389/tcp)**<br><br>Сертификат X.509 в цепочке сертификатов не подписан уполномоченным органом сертификации.<br><br>**CVSS Base Score: 6.4**<br>**CVSS Vector Score: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N** | Покупка или генерация соответствующего сертификата для данного сервера |
| Microsoft Windows Remote Desktop Protocol Server подвержен Man-in-the-Middle уязвимостям<br><br>Дополнительные ссылки по данной уязвимости:<br>http://www.oxid.it/downloads/rdp-gbu.pdf<br>http://www.nessus.org/u?e2628096<br>http://technet.microsoft.com/en-us/library/cc782610.aspx<br><br>**CVSS Base Score: 5.1**<br>**CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P**<br>**CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:ND** | • Использовать SSL в качестве транспортного уровня для этой службы(если поддерживается)<br>• Включить параметр «Разрешение подключения только с компьютеров которые поддерживают авторизацию на уровне сети (NLA)» если это возможно. |

| | |
|---|---|
| **CVSS Temporal Score: 4.6**<br><br>cve:CVE-2005-1794<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1794 | |
| Удаленная служба поддерживает использование шифра RC4.<br><br>Удаленный хост поддерживает использование RC4 в одном или нескольких наборах шифров. Шифр RC4 имеет недостатки в генерации псевдослучайного потока байтов<br><br>Если открытый текст зашифрован неоднократно (например HTTP cookies) и атакующий может получит много шифртекстов, есть вероятность получить данные в открытом виде<br><br>Ссылки по данной уязвимости:<br>http://www.nessus.org/u?217a3666<br>http://cr.yp.to/talks/2013.03.12/slides.pdf<br>http://www.isg.rhul.ac.uk/tls/<br><br>CVSS Base Score: 2.6<br>CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N<br>CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:C<br>CVSS Temporal Score: 2.2<br><br>cve:CVE-2013-2566<br>http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566 | Перенастройка службы или приложения, если это возможно, на использование другого шифра |
| **Уровень шифрования службы терминалов не соответствует FIPS-140**<br><br>**CVSS Base Score: 2.6**<br>**CVSS Vector Score: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N** | Изменить уровень RDP шифрования на FIPS-140 |

## 6. Прикладное программное обеспечение

| Текущее состояние | Оптимальная структура | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| Уровень сложности доступа постороннего лица к интерфейсу, ссылкам, ярлыкам входа, установленным подключениям к базам производственных программ | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Ярлыки для подключения программ находятся на рабочем столе пользователей.<br>Настроена автоблокировка рабочих станций. | <Описывается оптимальная структура><br>**Например:**<br>1.Все базы производственных программ должны защищаться паролем<br>2.Должна быть политика автоблокировки рабочих станций пользователей, которая не позволит злоумышленнику получить доступ к базам спец программ | <Описываются текущие проблемы на объекте><br>**Например:**<br>База без пароля | <Описываются текущие проблемы на объекте><br>**Например:**<br>Исправить ошибки |
| Результат проверки соответствия паролей на специализированное бухгалтерское либо иное производственное ПО международным критериям криптозащиты | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Пароли к спец ПО соответствуют международным критериям криптозащиты | <Описывается оптимальная структура><br>**Например:**<br>Пароль должен быть не менее 6 символов, содерджать буквы верхнего и нижнего регистра а также цифры | <Описываются текущие проблемы на объекте><br>**Например:**<br>Замечания отсутствуют | <Описываются текущие проблемы на объекте><br>**Например:**<br>Замечания отсутствуют |
| Наличие возможности физической распечатки информации, находящейся в базах спец ПО лицами, не имеющими разрешения на доступ к ней | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>На файловом хранилище находятся сканы документов доступные под правами гостя | <Описывается оптимальная структура><br>**Например:**<br>1.Все важные документы должны разграничиваться правами доступа, по возможности шифроваться | <Описываются текущие проблемы на объекте><br>**Например:**<br>Сканированные документы компании в свободном доступе | <Описываются текущие проблемы на объекте><br>**Например:**<br>.По возможности использовать шифрование для важных документов |

## 7. Организационное обеспечение

| Текущее состояние | Оптимальная структура* | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| Возможность доступа к включенной рабочей станции, периферийному оборудованию посторонним лицом либо другим пользователем при отсутствии сотрудника на рабочем месте (вышел по необходимости, на обед, на перекур и т.д.) | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>На всех компьютерах домена работает автоблокировка<br>Некоторое сетевое оборудование находится в свободном доступе. | <Описывается оптимальная структура><br>**Например:**<br>1.Регламентирование политики безопасности рабочих мест и периферийного оборудования<br>2.Проведение вступительных и плановых обучений по безопасности рабочих станций | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Отсутствие регламентированных политик безопасности рабочих мест и периферийных устройств<br>2.Отсутствие вступительных и плановых учений по безопасности рабочих станций | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Внедрение регламентированных политик безопасности рабочих мест при отсутствии сотрудника<br>2.Проведение вступительных и плановых обучений по безопасности рабочих станций |
| Возможности получения доступа к операционной системе пользователем в ночное и нерабочее время | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Практически все пользователи выключают компьютеры на ночь | <Описывается оптимальная структура><br>**Например:**<br>1.Компьютеры должны выключатся на ночь<br>2.Кабинеты с рабочими стациями должны закрываться на ночь<br>3.Необходимо регламентировать и документировать доступы к компьютерам через удаленное подключение | <Описываются текущие проблемы на объекте><br>**Например:**<br>1. Отсутствует документация и регламенты по удаленному доступу к рабочим станциям | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Внедрение ИТ регламента удаленного доступа к рабочим стациям а также ведение документации по этим доступам. |
| Вероятность утечки конфиденциальных данных через бумажные либо иные несанкционированные носители | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Практически у всех пользователей разрешен запуск съёмных флэш устройств. Некоторые пользователи хранят пароли на рабочем столе | <Описывается оптимальная структура><br>**Например:**<br>1.Возможность запуска съемных флэш носителей должна быть максимально ограничено<br>2.Должна присутствовать политика «чистого стола». Политика чистого стола/чистого экрана снижает риски неразрешенного доступа,<br>потери и повреждения информации в течение стандартного рабочего дня и в нерабочее время<br>3.Необходимо иметь соответствующий ИТ регламент по работе со сменными и бумажными носителями | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Доступ к сменным носителям есть практически у всех пользователей<br>2. Отсутствует политика «Чистого стола»<br>3.Отсутствует ИТ регламент по работе со сменными и бумажными носителями | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Ограничить возможность запуск съемных флэш носителей только тем пользователям, для которых этот доступ действительно необходим. |
| Учет, мониторинг и отчетность действий пользователей в серверной структуре и система оповещений администратора о нарушениях | | | |

| безопасности в серверной структуре | | | |
|---|---|---|---|
| <Описывается текущее состояние на объекте><br>**Например:**<br>Мониторинга действий пользователя в серверной структуре отсутствует. | <Описывается оптимальная структура><br>**Например:**<br>1.На ОС серверов и общих ресурсов должно быть реализовано ведение логов, источника и времени логина, времени работы пользователей в разрезе по доменному уникальному логину пользователя. Доступ к лог-файлам имеет сетевой администратор, генеральный директор и руководитель отдела ИТ-безопасности.<br>2.Должна присутствовать система комплексного мониторинга и оперативного оповещения нарушения нормального состояния всех общедоступных ресурсов, работа которых важна для Компании. | <Описываются текущие проблемы на объекте><br>**Например:**<br>Любые нарушения периметра безопасности либо неразрешенные действия пользователя (удаление файла, базы, перекачка файла на внешний носитель и т.д.) останутся незаметными для ответственных лиц. | <Описываются текущие проблемы на объекте><br>**Например:**<br>1.Внедрение системы полного учета действий пользователей в серверной среде |
| Возможность утечки информации и возможности заражения системы пользователем через интернет и web-контент | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>В сети используется прокси сервер который блокирует опасные сайты | <Описывается оптимальная структура><br>**Например:**<br>1.Пользователям должен быть максимально закрыт доступ к нежелательным сайтам в том числе файлообменникам.<br>2. Необходимо иметь ИТ регламент регулирующий права пользователей а также необходимые действия при заражении компьютера вредоносным ПО<br>3. Необходимо проводить вступительное и плановое обучение пользователей по соответствующему регламенту. | <Описываются текущие проблемы на объекте><br>**Например:**<br>Отсутствует ИТ регламент регулирующий права и обязанности пользователей | <Описываются текущие проблемы на объекте><br>**Например:**<br>ИТ отделу необходимо составить и утвердить регламент регулирующий права и обязанности пользователей |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .
- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

## 8. Нормативное обеспечение

<table>
<tr><th>Объект изучения</th><th>Текущее состояние</th><th>Оптимальная структура*</th></tr>
<tr><td>Документы, регулирующие права и обязанности сотрудников в ИТ-сфере компании</td><td>Такие документы в утвержденном виде отсутствуют</td><td rowspan="6">Должны быть подготовлены документированные процедуры для видов системной деятельности, связанной со средствами обработки информации и средствами обмена информацией, такими как:<ul><li>процедуры запуска и прекращения работы компьютера;</li><li>резервное копирование ;</li><li>обслуживание оборудования , обращение с носителями информации;</li><li>менеджмент компьютерной комнаты и обработки корреспонденции; безопасность.</li></ul>Процедуры эксплуатации должны определять инструкции по подробному<br>исполнению каждой работы, включая следующее:<br>1.Обработка информации и обращение с информацией;<br>2. Резервное копирование ;<br>3.Планирование требований , включая взаимозависимости с другими системами, время начала самой ранней работы и время завершения самой поздней работы;<br>4. Инструкции по обращению с ошибками или другими исключительными условиями, которые могут возникнуть в ходе выполнения работы, включая ограничения на использование системных утилит;<br>5. Служебные контакты на случай неожиданных эксплуатационных или технических трудностей;<br>6.Специальные инструкции по выводу информации и по обращению с носителями информации , например , использование специальных канцтоваров или управление выводом конфиденциальной информации , включая процедуры безопасной ликвидации вывода информации неудавшихся работ.<br>7.Повторный пуск системы и процедуры восстановления для использования в случае сбоя в работе системы ;<br>8.Менеджмент информации контрольного и системного журналов<br>С процедурами эксплуатации, а также с документированными процедурами для<br>видов системной деятельности надо обращаться как с официальными документами, и изменения должны санкционироваться руководством. Там , где это технически</td></tr>
<tr><td>Документы, регулирующие уровни и возможности доступа к ресурсам</td><td>Такие документы в утвержденном виде отсутствуют.</td></tr>
<tr><td>Документы, регулирующие уровни физической безопасность помещений и структуры</td><td>Существует общий регламент безопасности помещений и структуры.</td></tr>
<tr><td>Документы, регулирующие ИТ-безопасность рабочих мест</td><td rowspan="2">В компании существует соответствующие документы которые регламентированы</td></tr>
<tr><td>Документы, регулирующие безопасность данных, уровни доступа к ним</td></tr>
<tr><td>Документы, обозначающие уровень ответственности и санкций в случае нарушений</td><td>Такие документы в компании отсутствуют.</td></tr>
</table>

| | | |
|---|---|---|
| | | выполнимо, информационные системы должны управляться последовательно, используя одни и те же процедуры, инструментальные средства и утилиты . |

*Оптимальная структура формируется на основании следующих стандартов:

- ГОСТ Р ИСО/МЭК ТО 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК ТО 13335-2 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО – 13335-4 – 2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
- ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасной сети».
- ГОСТ Р ИСО/МЭК ТО 177799 – 2005 «Информационная технология. Практические правила управления информационной безопасностью.
- ISO/IEC27001 – «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» .
- ISO/IEC27002 – «Информационные технологии. Свод правил по управлению защитой информации».

## 9. Корпоративные данные

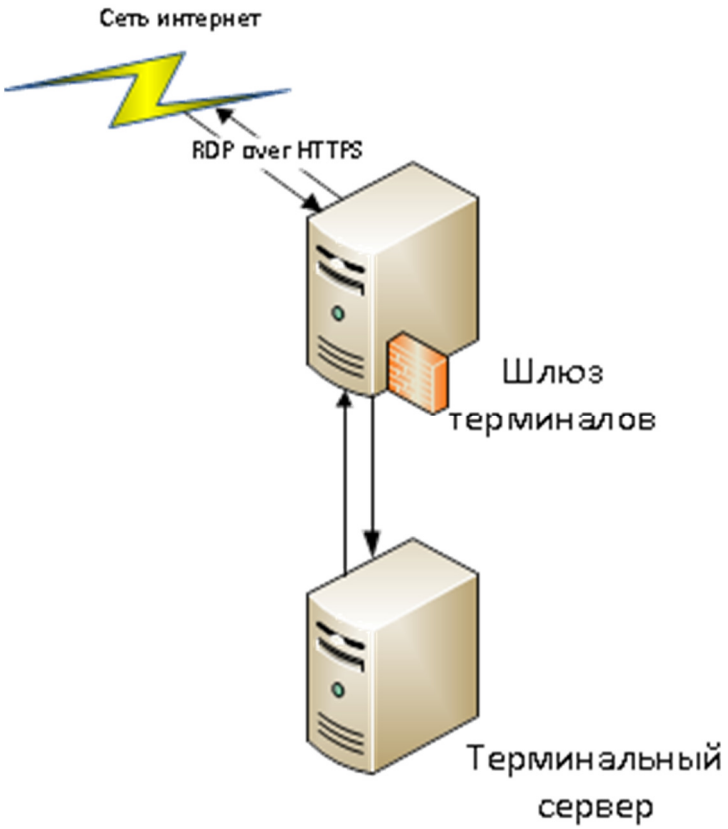
| Текущее состояние | Оптимальная структура | Нарушения, замечания и угрозы | Меры по исправлению ситуации |
|---|---|---|---|
| Уровень ограничений доступа и защищенности корпоративных данных, файловых данных, таблиц, документов, баз данных от намеренных либо случайных действий, как сотрудников Компании так и посторонних лиц | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>У пользователей присутствуют разграничение прав для документов на сетевом хранилище | <Описывается оптимальная структура><br>**Например:**<br>1.Наличие системы мониторинга пользователей<br>2.Наличие системы версионности документов<br>3.Наличие системы шифрования документов<br>4.Наличие системы документооборота, наличие четко регламентированных требований документообороту | <Описываются текущие проблемы на объекте><br>**Например:**<br>Отсутствует шифрование документов<br>Отсутствуют четко регламентированные требования по документообороту | <Описываются текущие проблемы на объекте><br>**Например:**<br>Установка и конфигурирование системы мониторинга пользователей |
| Результат проверки возможности недобросовестным сотрудником намеренного перемещения ключевой информации за пределы офиса корпоративных данных, файловых данных, таблиц, документов, баз данных | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Пользователи имеют неограниченный доступ к съёмным устройствам | <Описывается оптимальная структура><br>**Например:**<br>Пользователи должны иметь минимальные права доступа к тем или иным документам<br>Пользователи должны иметь ограниченный доступ к съёмным устройства | <Описываются текущие проблемы на объекте><br>**Например**<br>Любой электронный документ к которому пользователь имеет доступ можно вынести за пределы офиса | <Описываются текущие проблемы на объекте><br>**Например:**<br>Внедрить систему систему шифрование файлов для возможности работы с ними только в офисной сети компании. |
| Наличие возможности умышленного получения доступа к корпоративным данным, файловым данных, таблиц, документов, баз данных посторонними лицами | | | |
| <Описывается текущее состояние на объекте><br>**Например:**<br>Получить доступ к корпоративным данным может любой пользователь | <Описывается оптимальная структура><br>**Например:**<br>Доступ к любым корпоративным данным, файловым данным, таблицам, документам, баз данным должен быть ограничен используя программные и аппаратные средства защиты | <Описываются текущие проблемы на объекте><br>**Например**<br>Свободный доступ к сети интернет | <Описываются текущие проблемы на объекте><br>**Например:**<br>Запретить доступ к конфиденциальным данным компании через гостевой доступ |

## 10. Внутренняя IT-структура – СКС, внутрисетевые устройства, коммутационные устройства.

| № | IP адрес | Название устройства | Описание |
|---|---|---|---|
| 1 | 133.12.2.12 | 3COM Switch 4200G Gigabit Family | Серверная 1 |
| 2 | 133.12.4.12 | 3COM Switch 42xxG Gigabit Family | Серверная 1 |
| 3 | 133.12.7.12 | 3COM Switch 42xxG Gigabit Family | Серверная 1 |
| 4 | 133.12.9.12 | 3COM Switch 42xxG Gigabit Family | Серверная 2 |
| 5 | 133.12.244.12 | 3COM Switch 42xxG Gigabit Family | Серверная 1 |
| 6 | 133.12.4.12 | 3COM Switch 42xxG Gigabit Family | Серверная 1 |
| 7 | 133.12.23.12 | 3COM Switch 42xxG Gigabit Family | Серверная 1 |
| 8 | 133.12.22.12 | 3COM Switch 42xxG Gigabit Family | Серверная 2 |

**Логическая схема сети**

**Например:**



## 11. Серверное оборудование – аппаратная часть

| Точные модели серверного оборудования | Роль оборудования в системе, краткое описание функциональных задач | Основные параметры производительности и комплектации | Описание административных доступов и прав | Замечания и рекомендации по приведению к стандартам |
|---|---|---|---|---|
| HP Proliant DL360 | Exchange | E5620/16GB/137GB, 500GB | ФИО и административный доступ | Необходимо вынести серверную структуру в отдельный VLAN |
| HP Proliant DL360 | Резервный контроллер домена,DNS | E5620/16GB/137GB, 500GB | ФИО и административный доступ | Необходимо вынести серверную структуру в отдельный VLAN |
| HP Proliant DL360 | Основной контроллер домена,DNS | E5620/16GB/137GB, 500GB | Д ФИО и административный доступ | Необходимо вынести серверную структуру в отдельный VLAN |

## 12. Сервера – логическая часть

| Логическое имя сервера | Основные серверные роли | Оценка критичности узла, методы обеспечения отказоустойчивости, максимальное время простоя (с точки зрения пользователей и руководства) | Наличие резервных копий, конфигурация глубины архива и расписания выполнения | Замечания и рекомендации по приведению к стандартам |
|---|---|---|---|---|
| Serrver1 (физический носитель) ОС: 2008R2 | Exchange | Высокая критичность | Ежедневно используя Acronis 11. В воскресенье полный, ежедневно диффиренциальный | Необходимо принять меры для резервирования ролей данного сервера |
| Serrver2 (физический носитель) ОС: 2008 | Резервный контроллер домена,DNS,SQL | Высокая критичность | Ежедневно используя Acronis 11. В воскресенье полный, ежедневно диффиренциальный | Необходимо принять меры для резервирования ролей данного сервера |
| Serrver3 (физический носитель) ОС: 2008 | Основной контроллер домена,DNS | Высокая критичность | Ежедневно используя Acronis 11. В воскресенье полный, ежедневно диффиренциальный | Замечания отсутствуют |

## 13. Сервера – производительность и доступ

| Логическое имя сервера | Процент постоянной загрузки основных ресурсов*:<br>Процессорное время<br>Оперативная память<br>Нагрузка I\O | | | | Описание узких мест производительности | Описание административных доступов и прав | Замечания и рекомендации по приведению к стандартам |
|---|---|---|---|---|---|---|---|
| | % загруженности процессора | Свободно оперативной памяти,% | Количество обращений к диску/с(iops) | Длина очереди диска | | | |
| Serrver1 (физический носитель)<br>ОС: 2008R2 | 2,5 | 13% | 11 | 0,1 | Слишком мало свободной оперативной памяти. Microsoft рекомендует не менее 25% | ФИО и административный доступ | Увеличить количество оперативной памяти |
| Serrver2 (физический носитель)<br>ОС: 2008 | 2 | 9% | 45 | 0,11 | Слишком мало свободной оперативной памяти. Microsoft рекомендует не менее 25% | ФИО и административный доступ | Увеличить количество оперативной памяти |
| Serrver3 (физический носитель)<br>ОС: 2008 | 13 | 73% | 4,4 | 0,6 | Отсутствуют | ФИО и административный доступ | Отсутствуют |
| | | | | | | | |
| | | | | | | | |

*показатели снимаются только для серверов под управлением MS Windows

## 14. Пользовательская структура

| | |
|---|---|
| | Все в порядке. |
| | Обратить внимание. |
| | Проблема. Необходимо принимать меры. |

| Роль пользователя и исполь-зуемое ПО | Наличие прав адми-нис-тратора | Лицензии рабочего места | Аппаратное обеспечение | Актуаль-ность антивируса | Актуаль-ность обновлений ПО | Наличие копии рабочих документов локально | Наличие бумажных носителей с паролями и конф. данными на рабочем месте | Рекламации и пожелания пользователя |
|---|---|---|---|---|---|---|---|---|
| **Компьютер 1 ( ФИО Пользоватея)** | | | | | | | | |
| Сотрудник 1<br>**ПО:**<br>word, excel, outlook | Нет | Radmin Server 3.5<br>Kaspersky Endpoint Security 10 для Windows [Русский (Россия)] | **Тип ЦП**:<br>QuadCore Intel Core, 2900 MHz<br>**Системная плата:**<br>Asus P8H61-I (<br>**Чипсет системной платы:**<br>Intel Cougar Point<br>**Системная память:**<br>4007 МБ | актуально | актуально | присутствуют | Нет | Отсутствуют |
| **Компьютер 2 ( ФИО Пользоватея)** | | | | | | | | |
| Сотрудник 1<br>**ПО:**<br>word, excel, outlook | Нет | Radmin Server 3.5<br>Kaspersky Endpoint Security 10 для Windows [Русский (Россия)] | **Тип ЦП**:<br>QuadCore Intel Core, 2900 MHz<br>**Системная плата:**<br>Asus P8H61-I (<br>**Чипсет системной платы:**<br>Intel Cougar Point<br>**Системная память:**<br>4007 МБ | актуально | актуально | присутствуют | Нет | Отсутствуют |
| **Компьютер 3( ФИО Пользоватея)** | | | | | | | | |
| Сотрудник 1<br>**ПО:**<br>word, excel, outlook | Нет | Radmin Server 3.5<br>Kaspersky Endpoint Security 10 для Windows [Русский (Россия)] | **Тип ЦП**:<br>QuadCore Intel Core, 2900 MHz<br>**Системная плата:**<br>Asus P8H61-I (<br>**Чипсет системной платы:**<br>Intel Cougar Point<br>**Системная память:**<br>4007 МБ | актуально | актуально | присутствуют | Нет | Отсутствуют |
| **Компьютер 4 ( ФИО Пользоватея)** | | | | | | | | |
| Сотрудник 1<br>**ПО:**<br>word, excel, outlook | Нет | Radmin Server 3.5<br>Kaspersky Endpoint Security 10 для Windows [Русский (Россия)] | **Тип ЦП**:<br>QuadCore Intel Core, 2900 MHz<br>**Системная плата:**<br>Asus P8H61-I (<br>**Чипсет системной платы:**<br>Intel Cougar Point<br>**Системная память:**<br>4007 МБ | актуально | актуально | присутствуют | Нет | Отсутствует |
| **Компьютер 5 ( ФИО Пользоватея)** | | | | | | | | |
| Сотрудник 1<br>**ПО:**<br>word, excel, outlook | Нет | Radmin Server 3.5<br>Kaspersky Endpoint Security 10 для Windows [Русский (Россия)] | **Тип ЦП**:<br>QuadCore Intel Core, 2900 MHz<br>**Системная плата:**<br>Asus P8H61-I (<br>**Чипсет системной платы:** | актуально | актуально | присутствуют | Нет | Отсутствуют |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Intel Cougar Point<br>**Системная память:**<br>4007 МБ | | | | | |

## 15. Модель зрелости по методологии COBIT:

На основании полученых данных описывается модель зрелости по методологии COBIT
**Например:**

1. **Оценка и управление ИТ рисками**

Управление процессом «Оценка и управление ИТ рисками» удовлетворяет следующим бизнес требованиям к ИТ анализ и информирование об ИТ рисках и их потенциальном воздействии на бизнес процессы и цели и соответствует характеристикам:

***Начальный***

На ИТ риски обращают внимание от случая к случаю. Проводятся неформальные оценки рисков, определяемые каждым отдельным проектом. Как правило, оценки рисков иногда включаются отдельно в план выполнения проекта, но ответственность за их проведение редко возлагается на конкретных менеджеров. Специфические риски, относящиеся к ИТ, такие как безопасность, достоверность и целостность, иногда учитываются при выполнении отдельных проектов. Информационные риски, влияющие на текущую операционную деятельность, иногда обсуждаются на совещаниях руководства. Если риски учитываются, то меры по их минимизации непоследовательны. Возникает понимание того, что ИТ риски важны и должны учитываться.

2. **Определение и управление уровнем обслуживания**

Управление процессом «Определение и управление уровнем обслуживания» удовлетворяет следующим бизнес требованиям к ИТ обеспечение соответствия между основными ИТ у слугами и корпоративной стратегией и соответствует характеристикам:

***Начальный***

Есть осознание необходимости управления уровнем услуг, однако, этот процесс пока неформален и, фактически, является лишь реакцией на происходящие события. Ответственность и отчетность по предоставлению услуг определены на неформальном уровне. Если показатели оказания услуг и существуют, то они носят качественный характер при нечетком определении конечных целей. Отчетность является неформальной, нерегулярной и непоследовательной.

3. **Обеспечение непрерывности ИТ сервисов**

Управление процессом «Обеспечение непрерывности ИТ сервисов» удовлетворяет следующим бизнес требованиям к ИТ минимизация последствий для организации в случае сбоя в оказании ИТ услуг и соответствует характеристикам:

***Начальный***

Ответственности по обеспечению непрерывности услуг не формализованы, полномочия ответственных лиц ограничены. Руководство начинает осознавать риски, связанные с потребностью обеспечении непрерывного предоставления услуг. Основное внимание сосредоточено на обслуживании ресурсов инфраструктуры, а не на ИТ услугах. Пользователи применяют свои собственные приемы, чтобы справляться со сбоями в предоставлении ИТ услуг. Реакция службы ИТ на крупные сбои заранее не продумана и не подготовлена. Практикуются плановые отключения системы в целях ИТ обслуживания, без учета выполнения бизнес требований.

**4. Обеспечение безопасности систем**

Управление процессом «Обеспечение безопасности систем» удовлетворяет следующим бизнес требованиям
К ИТ обеспечение целостности информации и инфраструктуры обработки данных, а также минимизация
Последствий для бизнеса от инцидентов и уязвимостей в системе безопасности и соответствует характеристикам:

***Начальный***

Организация осознает необходимость в обеспечении безопасности ИТ. Однако степень этого осознания зависит от конкретных сотрудников. Меры по обеспечению безопасности ИТ, фактически, являются лишь реакцией на происходящие события и никак не оцениваются. В связи с неопределенной ответственностью при обнаружении случаев нарушения безопасности ИТ происходит реакция по типу «указывания пальцем». Реакции на случаи нарушения безопасности непредсказуемы.

**5. Обучение и подготовка пользователей**

Управление процессом «Обучение и подготовка пользователей» удовлетворяет следующим бизнес требованиям к ИТ эффективное использование приложений и технологических решений, а также обеспечение выполнения пользователями требований политик и процедур и соответствует характеристикам:

***Начальный***

Имеются факты, указывающие на то, что в организации осознали необходимость создания программы подготовки и обучения персонала, однако нет отлаженных процессов для решения данного вопроса. В условиях отсутствия организованной программы сотрудники самостоятельно находят нужные им курсы подготовки и посещают их. Некоторые из этих курсов дают подготовку по корпоративной этике, общим вопросам и практическим действиям по обеспечению безопасности систем. Подходы руководства к вопросам обучения не согласованы. Отсутствует систематическое обсуждение вопросов подготовки и обучения персонала, не выработаны подходы к решению этих вопросов.

**6. Управление службой технической поддержки и инцидентами**

Управление процессом «Управление службой технической поддержки и инцидентами» удовлетворяет следующим бизнес требованиям к ИТ эффективное использование ИТ систем путем анализа и решения проблем пользователей, вопросов и инцидентов и соответствует характеристикам:

***Определенный***

Осознана и признана необходимость создания службы поддержки пользователей и процесса управления инцидентами. Стандартизованы и документально оформлены процедуры. Обучение осуществляется на неформальном уровне. Однако решение вопросов обучения и соблюдения стандартов предоставлено отдельным сотрудникам. Разработана база данных на основе часто задаваемых вопросов, содержащая ответы на эти вопросы, подготовлены рекомендации для пользователей. Однако отдельные сотрудники должныискать ответы на вопросы и

могут не всегда следовать им. Отслеживание вопросов и проблем осуществляется вручную, текущий контроль ведется в отдельных случаях, отсутствует формализованная система отчетности. Не фиксируется время реагирования на возникшие вопросы и инциденты. Возможны ситуации, когда возникшие запросы и инциденты не решаются. Пользователи имеют четкие инструкции когда и как сообщать о проблемах и инцидентах.

# Выводы

## Физический контроль доступа в помещения, наблюдение за помещениями

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Аппаратное обеспечение информационной системы

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД

- Провести инвентаризацию
- И т.п

## Сетевое обеспечение информационной системы:

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Экспресс тесты безопасности

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Прикладное программное обеспечение

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Организационное обеспечение и  Корпоративные данные

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

eToken с привязкой к домену Заказчика для защиты подключения удаленных пользователей к корпоративной сети

## Нормативное обеспечение

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Серверная структура, СКС, внутрисетевые устройства, коммутационные устройства

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД
- Провести инвентаризацию
- И т.п

## Пользовательская структура

На основании полученной информации будут описаны общие выводы.

**Например**:

Физический контроль обеспечен частично. Некоторые серверные и коммутационные помещения недостаточно защищены

***Рекомендации:***

На основании полученных данных будут выведены общие рекомендации по устранению проблем безопасности

**Например:**

- Установить систему СКУД

- Провести инвентаризацию
- И т.п