**Вводные данные:**

Система выявления рисков ИБ (СВРИБ) обеспечивает проведение инвентаризации в отдельных сегментах сети и передачу данных на центральный сервер. Физически данный компонент размещается отдельно от центрального сервера.

ИС Локального узла СВРИБ предназначена для автоматизации следующих бизнес-процессов:

* Управление рисками ИБ в ООО «Саратовский Завод».

Контроль соответствия требованиям ИБ в процессе жизненного цикла в ООО «Саратовский Завод»

* Контроль защищенности ИТ-активов в ООО «Саратовский Завод»

Максимальный уровень конфиденциальности информации, обрабатываемой в Системе –конфиденциальная: {коммерческая тайна}.

Режим доступа к информации (отметить одно из представленных):

|  |  |  |
| --- | --- | --- |
|  | ☐ | Однопользовательская |
|  | ☒ | Многопользовательская |

Необходимость разграничения доступа к информации (отметить одно из представленных):

|  |  |  |
| --- | --- | --- |
|  | ☒ | Необходимо |
|  | ☐ | Нет необходимости |

Смежные системы: Microsoft Active Directory, САЗ (система антивирусной защиты).

В составе Системы отсутствует программное обеспечение, для которого в Компании разработан и утвержден профиль ИБ, Система к ЦОД не подключается.

В Системе предусматривается обработка только общедоступное ПДн работников. Доступ с мобильных устройств не предполагается. ПДн из Интернета не обрабатываются.

Угрозы информационной безопасности, связанные с наличием недекларированных возможностей в программном обеспечении признаны неактуальными.

Использование квалифицированной ЭП не планируется.

Класс защищённости системы – 1Г.

Перечень программных продуктов

| № | тип ПО | наименование ПО |
| --- | --- | --- |
|  | Операционная система сервера | Операционная система «Microsoft Windows 10 Professional» |
|  | Специализированное ПО | ПО «R-Vision SGRC» |
|  | Специализированное ПО, сканер уязвимости | XSpider |
|  | Система антивирусной защиты | Kaspersky Endpoint Security Total Security |
|  | Специализированное ПО, программа фиксации и контроля исходного состояния программного комплекса | ФИКС 2.0.2 |

## РЕШЕНИЯ ПО РЕАЛИЗАЦИИ ОБЩИХ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Максимальный уровень конфиденциальности информации, обрабатываемой в Системе, – конфиденциальная: {коммерческая тайна}.

Система удовлетворяет всем требованиям информационной безопасности регламентирующих документов Компании для возможности обработки информации максимального уровня конфиденциальности - конфиденциальная.

Система обеспечивает защиту от несанкционированного доступа (НСД) на уровне не ниже установленного требованиями, предъявляемыми к классу защищенности 1Г автоматизированных систем (АС) по классификации действующего руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Средства вычислительной техники Системы, подключаемые к корпоративной сети Компании, размещаются в локальных вычислительных сетях, в которых выполнены требования Положения Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему». В случае использования каналов связи, выходящих за пределы контролируемой зоны, применяются защищенные каналы связи, защищенные волоконно-оптические линии связи либо средства криптографической защиты информации.

Обеспечена своевременная установка обновлений информационной безопасности на прикладное и системное программное обеспечение компонент Системы.

На компонентах Системы установлены антивирусные средства, соответствующие требованиям Положения Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему».

Аутентификация и авторизация пользователей Системы осуществляется с использованием службы корпоративного каталога на базе Microsoft Active Directory (случаи невозможности интеграции со службой корпоративного каталога должны быть согласованы с подразделениями ИТ и ИБ). Для доступа к Системе используется механизм единого входа – SSO (single sign-on), основанный на доменной аутентификации.

Доступ к Системе привилегированных пользователей осуществляется через Систему контроля действий привилегированных пользователей (СКДПП), при отсутствии возможности использования СКДПП – через терминальный сервер, развернутый либо в составе Системы, либо в составе смежной ИС.

В Системе реализована ролевая модель разграничения доступа. Различным группам пользователей назначаются различные права доступа в Системе, в рамках их должностных обязанностей, в соответствии с Регламентом предоставления доступа, а также с соблюдением принципов «минимально необходимых привилегий» (least privilege) и «минимально необходимых знаний» (need to know).

Реализованные в Системе ограничения на использование средств аутентификации (пароли, PIN-коды и т.п.), обеспечивают выполнение требований к длине, сложности, сроку действия, установленные Стандартом Компании «Политики информационной безопасности».

Срок хранения информации о событиях ИБ в журналах аудита Системы составляет: [90] дней. По истечении указанного срока журналы архивируются и хранятся на протяжении [365] дней.

Применение для программного обеспечения Системы утвержденных профилей ИБ в настоящее время не требуется, поскольку в составе Системы отсутствует профиль ИБ.

Компоненты Системы размещены в сегменте внутренней ДМЗ. Доступ к внутренним ДМЗ из сетей, не соответствующих требованиям Положения Компании, осуществляется с использованием защищенных протоколов с шифрованием (SSL, SFTP и т.п.), соответствующих требованиям к СКЗИ.

В Системе предусматривается обработка только персональных данных (ПДн) работников, включенных в общедоступные источники персональных данных Компании (в том числе справочники, адресные книги).

Согласно Положению Компании «Обеспечение информационной безопасности в информационных системах персональных данных», необходимый уровень защищенности персональных данных достигается применением мер, установленных для информационных систем, осуществляющих обработку информации для внутреннего пользования.

Сводная информация по реализации в Системе требований информационной безопасности для информационных систем (ИС) класса 1Г представлена в таблице ниже.

Таблица 20

Реализация требований к защите информации Системы от НСД (требования для АС класса 1Г)

| Требования к классу защищенности | Реализация требований ИБ | |
| --- | --- | --- |
| штатными средствами защиты информации прикладного и общесистемного ПО системы | другими средствами защиты информации |
| 1 | 2 | 3 |
| Подсистема управления доступом | | |
| Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов | **На уровне ОС Microsoft Windows 10 Professional:**  Идентификация и аутентификация привилегированных пользователей при подключении по RDP осуществляется штатными средствами ОС по доменным персонифицированным учетным записям (УЗ). | Доступ пользователей осуществляется с использованием системы контроля доступа (СКД) и антивирусной защиты Kaspersky Endpoint Security Total Security. Также применяются двухфакторная аутентификация (2FA) и система управления учетными записями (IAM) для усиления безопасности доступа. |
| Подсистема регистрации и учета | | |
| Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.  В параметрах регистрации указываются:   1. Дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы. 2. Результат попытки входа: успешная или неуспешная – несанкционированная. 3. Идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа. | Осуществляется средствами журналирования ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Применяются механизмы регистрации событий безопасности, доступные в Kaspersky Security Center. Данные регистрируются и хранятся в центральном журнале событий. | Для обеспечения дополнительного уровня безопасности применяется централизованная система управления логами, такая как Splunk или ELK Stack, для сбора и анализа данных событий безопасности. Также используются системы обнаружения вторжений (IDS) для мониторинга и анализа подозрительной активности. |
| Должен осуществляться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнал (учетную карточку). | Учет носителей информации осуществляется средствами Microsoft System Center Configuration Manager (SCCM), который позволяет отслеживать и управлять устройствами и носителями в корпоративной сети. Все носители маркируются и их данные заносятся в централизованный реестр. | Дополнительно применяются системы для управления и отслеживания носителей информации, такие как Varonis Data Security Platform, которые позволяют проводить аудит и контроль использования носителей. Используются процедуры периодической инвентаризации и проверки состояния носителей информации. |
| Подсистема обеспечения целостности | | |
| Должен осуществляться контроль целостности программных средств СЗИ НСД, а также неизменность программной среды.  При этом, целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ; целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации. | Контроль целостности программных средств СЗИ НСД и неизменность программной среды осуществляется средствами Kaspersky Endpoint Security Total Security, обеспечивающими вычисление и проверку контрольных сумм файлов на основе эталонных значений. Дополнительно используются встроенные функции ОС Microsoft Windows 10 Professional для проверки целостности системных файлов. | Реализованы механизмы контроля целостности с использованием специализированного ПО, такого как Tripwire или аналогичных средств мониторинга целостности. Также применяются регулярные аудиты и тестирование целостности данных с использованием инструментов резервного копирования и восстановления. |
| Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время. | Физическая охрана осуществляется с использованием систем контроля доступа (СКД) и видеонаблюдения, интегрированных в корпоративную сеть безопасности. Помещения, где размещены СВТ, оборудованы электронными замками и датчиками движения. | Дополнительно применяются меры физической безопасности, такие как охранные службы, регулярные патрули, а также сейфы и шкафы с усиленной защитой для хранения носителей информации. |
| Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД. | Тестирование функций СЗИ НСД проводится с использованием встроенных средств безопасности ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Регулярно выполняются сканирования на уязвимости и тестирование с использованием встроенных инструментов безопасности. | Для тестирования используются специализированные инструменты для проведения пентестов, такие как Metasploit, а также сторонние службы аудита и тестирования на проникновение. Применяются регулярные проверки и обновления политик безопасности. |
| Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. | Средства восстановления реализованы с использованием встроенных инструментов резервного копирования Windows Server и специализированного ПО для резервного копирования и восстановления данных, таких как Acronis Backup. Регулярно выполняется создание резервных копий и проверка их целостности. | Дополнительно используются внешние системы резервного копирования и восстановления, такие как облачные решения для резервного копирования (например, AWS Backup), и периодическое тестирование восстановления данных для проверки работоспособности резервных копий. |

Таблица 21

Реализация требований к защите информации Системы от НСД (требования для АС класса 1Г)

| Требования к классу защищенности | Реализация требований ИБ | |
| --- | --- | --- |
| штатными средствами защиты информации прикладного и общесистемного ПО системы | другими средствами защиты информации |
| 1 | 2 | 3 |
| Подсистема управления доступом | | |
| Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов | **На уровне ОС Microsoft Windows 10 Professional:**  Идентификация и аутентификация привилегированных пользователей при подключении по RDP осуществляется штатными средствами ОС по доменным персонифицированным учетным записям (УЗ). | Доступ пользователей осуществляется с использованием системы контроля доступа (СКД) и антивирусной защиты Kaspersky Endpoint Security Total Security. Также применяются двухфакторная аутентификация (2FA) и система управления учетными записями (IAM) для усиления безопасности доступа. |
| Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ | Реализуется средствами ОС Microsoft Windows 10 Professional: Идентификация терминалов осуществляется по номеру терминала, идентификация ЭВМ - по MAC-адресу. | Дополнительно используется управление сетью с применением коммутаторов и маршрутизаторов, поддерживающих идентификацию по IP и MAC-адресам. |
| Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам | Реализуется средствами файловой системы и встроенной системой безопасности ОС Windows: идентификация всех объектов осуществляется по именам файлов и каталогов. | Для дополнительной защиты используется программное обеспечение, такое как Tripwire, для мониторинга целостности файловой системы и идентификации изменений. |
| Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа | Контроль доступа осуществляется средствами Windows Server и R-Vision SGRC. Принятие решения о запрете или разрешении доступа субъекта к объекту производится на основе матрицы доступа и установленных политик безопасности. | Дополнительно используется многоуровневый контроль доступа с применением ролевых моделей (RBAC) и принципов минимально необходимых привилегий (least privilege). |
| Подсистема регистрации и учета | | |
| Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:   1. Дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы. 2. Результат попытки входа: успешная или неуспешная – несанкционированная. 3. Идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа. | Осуществляется средствами журналирования ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Применяются механизмы регистрации событий безопасности, доступные в Kaspersky Security Center. Данные регистрируются и хранятся в центральном журнале событий. | Для обеспечения дополнительного уровня безопасности применяется централизованная система управления логами, такая как Splunk или ELK Stack, для сбора и анализа данных событий безопасности. Также используются системы обнаружения вторжений (IDS) для мониторинга и анализа подозрительной активности. |
| Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:   1. Дата и время выдачи (обращения к подсистеме вывода). 2. Спецификация устройства выдачи [логическое имя (номер) внешнего устройства]. 3. Краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа. 4. Идентификатор субъекта доступа, запросившего документ. | Реализация регистрации выдачи печатных документов осуществляется средствами ОС Windows и ПО Kaspersky Endpoint Security Total Security. Средства журналирования фиксируют все действия по печати документов, указывая параметры регистрации. | Дополнительно используются средства управления печатью и контроля доступа к принтерам, такие как PaperCut, которые регистрируют все запросы на печать и обеспечивают детальный аудит печатной активности. |
| Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:   1. Дата и время запуска; 2. Имя (идентификатор) программы (процесса, задания); 3. Идентификатор субъекта доступа, запросившего программу (процесс, задание); 4. Результат запуска (успешный, неуспешный - несанкционированный). | Осуществляется средствами журналирования ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Применяются механизмы регистрации событий безопасности, доступные в Kaspersky Security Center. Данные регистрируются и хранятся в центральном журнале событий. | Для дополнительного уровня безопасности применяется централизованная система управления логами, такая как Splunk или ELK Stack, для сбора и анализа данных событий безопасности. Также используются системы обнаружения вторжений (IDS) для мониторинга и анализа подозрительной активности. |
| Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:   1. Дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная. 2. Идентификатор субъекта доступа. 3. Спецификация защищаемого объекта [логическое имя (номер)]. | Реализуется средствами ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Журналирование всех попыток доступа осуществляется средствами ОС Windows и антивирусного ПО. Данные регистрируются и хранятся в центральном журнале событий. | Для обеспечения дополнительного уровня безопасности применяется централизованная система управления логами, такая как Splunk или ELK Stack, для сбора и анализа данных событий безопасности. Также используются системы обнаружения вторжений (IDS) для мониторинга и анализа подозрительной активности. |
| Должен осуществляться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнал (учетную карточку). | Учет носителей информации осуществляется средствами Microsoft System Center Configuration Manager (SCCM), который позволяет отслеживать и управлять устройствами и носителями в корпоративной сети. Все носители маркируются и их данные заносятся в централизованный реестр. | Дополнительно применяются системы для управления и отслеживания носителей информации, такие как Varonis Data Security Platform, которые позволяют проводить аудит и контроль использования носителей. Используются процедуры периодической инвентаризации и проверки состояния носителей информации. |
| Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). | Реализуется средствами ОС Microsoft Windows 10 Professional, используя встроенные функции очистки оперативной памяти и внешних накопителей. Например, команды sdelete из пакета Sysinternals обеспечивают надежное удаление данных путем перезаписи. | Дополнительно применяются специализированные программы для безопасного удаления данных, такие как Eraser или BCWipe, которые обеспечивают многократную перезапись данных на освобождаемых участках памяти и накопителей, соответствуя требованиям стандартов безопасности. |
| Подсистема обеспечения целостности | | |
| Должен быть обеспечен контроль целостности программных средств СЗИ НСД, а также неизменность программной среды.  При этом целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ; целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации. | Контроль целостности программных средств СЗИ НСД и неизменность программной среды осуществляется средствами Kaspersky Endpoint Security Total Security, обеспечивающими вычисление и проверку контрольных сумм файлов на основе эталонных значений. Дополнительно используются встроенные функции ОС Microsoft Windows 10 Professional для проверки целостности системных файлов. | Реализованы механизмы контроля целостности с использованием специализированного ПО, такого как Tripwire или аналогичных средств мониторинга целостности. Также применяются регулярные аудиты и тестирование целостности данных с использованием инструментов резервного копирования и восстановления. |
| Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время. | Физическая охрана осуществляется с использованием систем контроля доступа (СКД) и видеонаблюдения, интегрированных в корпоративную сеть безопасности. Помещения, где размещены СВТ, оборудованы электронными замками и датчиками движения. | Дополнительно применяются меры физической безопасности, такие как охранные службы, регулярные патрули, а также сейфы и шкафы с усиленной защитой для хранения носителей информации. |
| Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД. | Тестирование функций СЗИ НСД проводится с использованием встроенных средств безопасности ОС Windows и антивирусного ПО Kaspersky Endpoint Security Total Security. Регулярно выполняются сканирования на уязвимости и тестирование с использованием встроенных инструментов безопасности. | Для тестирования используются специализированные инструменты для проведения пентестов, такие как Metasploit, а также сторонние службы аудита и тестирования на проникновение. Применяются регулярные проверки и обновления политик безопасности. |
| Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. | Средства восстановления реализованы с использованием встроенных инструментов резервного копирования Windows Server и специализированного ПО для резервного копирования и восстановления данных, таких как Acronis Backup. Регулярно выполняется создание резервных копий и проверка их целостности. | Дополнительно используются внешние системы резервного копирования и восстановления, такие как облачные решения для резервного копирования (например, AWS Backup), и периодическое тестирование восстановления данных для проверки работоспособности резервных копий. |