|  |  |
| --- | --- |
| Риски | Уровень |
| Вывод из строя; | Малый |
| Наличие в ПО недекларированных возможностей, оставленных для отладки, либо умышленно внедренных; | Малый |
| Ошибки кода и конфигурации ПО, активного сетевого оборудования; | Малый |
| Нарушение целостности исполняемых файлов; | Малый |
| Модификация ПО; | Малый |
| Отказы технических средств; | Малый |
| Проблемы с питанием технических средств; | Малый |
| Физическое повреждение технических средств, линий связи, сетевого и каналообразующего оборудования; | Малый |
| Несанкционированное изменение конфигурации активного сетевого оборудования и приемо-передающего оборудования; | Малый |
| Установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты; | Средний |
| Хищение технических средств и долговременных носителей конфиденциальной информации вследствие отсутствия контроля над их использованием и хранением. | Средний |
| Внедрение вирусов и других разрушающих программных воздействий; | Средний |
| перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика; | Средний |
| замена, вставка, удаление или изменение данных пользователей в информационном потоке; | Средний |
| вести, контролировать и проверять реестры носителей информации | Средний |
| перехват информации, передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации; | Средний |
| Использование уязвимостей ПО для взлома программной защиты с целью получения несанкционированного доступа к информационным ресурсам или нарушения их доступности; | Большой |
| Выполнение одним пользователем несанкционированных действий от имени другого пользователя; | Большой |
| Раскрытие, перехват и хищение секретных кодов и паролей; | Большой |
| Загрузка и установка в системе нелицензионного, непроверенного системного и прикладного ПО; | Большой |

Методы снижения рисков

|  |  |
| --- | --- |
| Метод | Оценка мероприятий |
| делать метки на носителях информации, отражающие уровень критичности содержащейся в них информации; | Низкая |
| уничтожать носители информации в соответствии с планом организации; | Низкая |
| доводить все руководящие документы до сотрудников; | Низкая |
| хранить диски в конвертах, коробках, металлических сейфах; | Низкая |
| не касаться поверхностей дисков, несущих информацию | Низкая |
| Осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света; | Низкая |
| Убирать диски и ленты, с которыми в настоящий момент не ведется работа; | Низкая |
| Хранить диски разложенными по полкам в определенном порядке; | Низкая |
| не давать носители информации с критической информацией неавторизованным людям; | Низкая |
| выбрасывать или отдавать поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры; | Низкая |
| уничтожать критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в организации; | Низкая |
| уничтожать распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком организации; | Низкая |
| обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру. | Низкая |
| Создание резервных копий | Средняя |
| обучать пользователей правильным методам очищения и уничтожения носителей информации; | Средняя |
| определение перечня информации, составляющей коммерческую тайну; | Средняя |
| ограничение доступа к информации, составляющей коммерческую тайну, | Средняя |
| путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка; | Средняя |
| учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана; | Средняя |
| регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров; | Средняя |
| нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства). | Средняя |
| общее регулирование доступа, включающее систему паролей и сегментацию винчестера; | Средняя |
| обучение персонала технологии защиты; | Средняя |
| обеспечение физической безопасности компьютера и магнитных носителей; | Средняя |
| выработка правил архивирования; | Средняя |
| хранение отдельных файлов в шифрованном виде; | Средняя |
| создание плана восстановления винчестера и испорченной информации. | Средняя |
| идентификация субъектов и объектов; | Высокая |
| разграничение доступа к вычислительным ресурсам и информации; | Высокая |
| контроль и регистрация действий с информацией и программами | Высокая |
| Использование антивирусного ПО | Высокая |
| отключать неиспользуемые терминалы; | Высокая |
| закрывать комнаты, где находятся терминалы; | Высокая |
| разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются; | Высокая |
| установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру | Высокая |
| использовать программы отключения терминала после определенного периода неиспользования; | Высокая |
| выключать систему в нерабочие часы; | Высокая |
| использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов. | Высокая |