Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Рабочие станции пользователей»

Уровень исходной защищённости ИСПДн

Документом ФСТЭК России «Методика актуализации угроз ПДн» вводится обобщенный показатель уровня исходной защищенности ИСПДн, зависящий от технических и эксплуатационных характеристик ИСПДн. «Рабочие станции пользователей» (коэффициент Y1).

* соответствии с заданными критериями оценки определяется уровень исходной защищенности ИСПДн «Рабочие станции пользователей»:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  | Уровень |  |  |
|  | Технические и эксплуатационные характеристики ИСПДн | | | | | | | | |  |  | защищеннос |  |  |
|  |  |  | ти |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | |  | |  |  | |  |  |  |  |  |
| 1. По территориальному | | | | | корпоративная | |  | распределенная | | |  | Средний | |  |
| размещению | | |  |  | ИСПДн, | охватывающая | | | многие | |  |  |
|  |  |  |  |  | подразделения одной организации | | | | | |  |  |  |  |
| 2. По | |  |  | наличию | ИСПДн, | имеющая | | одноточечный | | |  | Средний | |  |
| соединения | | | с | сетями | выход в сеть общего пользования | | | | | |  |  |
| общего пользования | | | | |  |  |  |  |  |  |  |  |  |  |
| 3. По | |  | встроенным | | - чтение, поиск; | | |  |  |  |  |  |  |  |
| (легальным) операциям с | | | | | - запись,удаление, сортировка; | | | |  |  |  | Низкий | |  |
| записями | | |  | баз | - модификация, передача | | | |  |  |  |  |
|  |  |  |  |  |  |  |
| персональных данных | | | | |  |  |  |  |  |  |  |  |  |  |
| 4. По | | разграничению | | | ИСПДн, к которой имеет доступ | | | | | |  |  |  |  |
| доступа к персональным | | | | | определенный | | перечень сотрудников | | | |  | Средний | |  |
| данным | |  |  |  | организации, являющейся владельцем | | | | | |  |  |
|  |  |  |  |  | ИСПДн, либо субъект ПДн | | | |  |  |  |  |  |  |
| 5. По | |  |  | наличию | Интегрированная | | |  | ИСПДн | |  |  |  |  |
| соединений | | | с | другими | (организация использует несколько баз | | | | | |  | Низкий | |  |
| базами | | ПДн | | иных | ПДн ИСПДн, при этом организация не | | | | | |  |  |
| ИСПДн | |  |  |  | является |  | владельцем | | всех | |  |  |  |  |
|  |  |  |  |  | используемых баз ПДн) | | | |  |  |  |  |  |  |
| 6. По уровню обобщения | | | | | ИСПДн, | в | которой | | данные | |  |  |  |  |
| (обезличивания) ПДн | | | | | обезличиваются только при передаче в | | | | | |  | Средний | |  |
|  |  |  |  |  | другие организации и не обезличены | | | | | |  |  |
|  |  |  |  |  | при предоставлении | | | пользователю в | | |  |  |  |  |
|  |  |  |  |  | организации | |  |  |  |  |  |  |  |  |
| 7. По | | объему | | ПДн, | ИСПДн, не предоставляющая никакой | | | | | |  | Высокий | |  |
| которые | |  |  |  | информации | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Уровень |  |  |
|  | Технические и эксплуатационные характеристики ИСПДн | | |  |  | защищеннос |  |  |
|  |  |  | ти |  |  |
|  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  |
| предоставляются | | |  | |  |  |  |  |
| сторонним | | |  | |  |  |  |  |
| пользователям ИСПДн | | |  | |  |  |  |  |
| без | | предварительной |  | |  |  |  |  |
| обработки | | |  | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Рабочие станции пользователей» оценивается как средний, поскольку не менее 70% характеристик ИСПДн (71%) соответствуют уровню «средний» или «высокий».

Согласно «Методики актуализации угроз ПДн» ФСТЭК России коэффициент исходной защищенности ИСПДн «Рабочие станции пользователей» Y1=5.

Описание угроз безопасности ПДн

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  | угроз |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Угрозы 1-го типа |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  | | |  |  | |  |  |  |  |  |
|  |  | 1. Угроза НСД | с |  | Внутренний | |  | Доступ в | операционную | среду |  | Технические | | |  | Нарушение | |  | Средняя | |  |  |
|  |  |  | нарушитель | |  | ИСПДн, | реализуемый | при |  | средства | ИСПДн | |  | конфиденциальн | |  | вероятность | |  |  |
|  |  | применением |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | помощи | эксплуатации | НДВ |  | (АРМ |  |  |  | ости, | |  |  |  |  |  |
|  |  | стандартных |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | (уязвимостей системного ПО), | | |  | пользователей, | | |  | целостностии | |  |  |  |  |  |
|  |  | функций |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | осуществляемый | | при |  | сервера |  |  |  | доступности | |  |  |  |  |  |
|  |  | операционной |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | физическом доступе к ИСПДн | | |  | приложений/БД | | |  | ПДн | |  |  |  |  |  |
|  |  | системы |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | или | средствам | ввода |  | ИСПДн) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информации в ИСПДн | |  |  | Программные | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | средства | ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | ОС |  |  |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное системное ПО надежных производителей.
2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник | |  |  | Способ реализации | | |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 1. | | | Не | осуществляется | | | | настройка | безопасности | | | ОС | на рабочих | | | станциях | |  |  |  |  |  |
|  |  |  |  |  |  |  | пользователей. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 2. | | | При покидании пользователем рабочего места не производится блокировка АРМ. | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  | 3. | | | Для | аутентификации | | | | используются слабые пароли, | | | | | настройки | | | парольной | |  |  |  |  |  |
|  |  |  |  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  | неуспешных попыток ввода пароля, не настроены параметры блокирования рабочей | | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  | станции после определенного периода неактивности. | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 2. Угроза | НСД с | |  |  | Внутренний | | |  | Реализуется путем эксплуатации | | | |  | Технические | |  |  | Нарушение | | |  | Средняя | |  |  |
|  |  |  |  | нарушитель | | |  | НДВ | в | системном | ПО |  | средства | ИСПДн: | |  | конфиденциальн | | |  | вероятность | |  |  |
|  |  | применением | | |  |  |  |  |  |  |  |  |
|  |  |  |  | Внешний | |  |  | (известных уязвимостей) | | |  |  | сервера |  |  |  | ости, |  |  |  |  |  |  |  |
|  |  | специально | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | | |  |  |  |  |  |  | приложений/БД | | |  | целостностии | | |  |  |  |  |  |
|  |  | созданных | для | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | этого программ | | |  |  |  |  |  |  |  |  |  |  |  | ИСПДн |  |  |  | доступности | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Программные | |  |  | ПДн |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | средства | ИСПДн: | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ОС |  |  |  |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное системное ПО надежных производителей.
2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 5. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |
|  |  |  |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | |  |  |  |  |  |  |  |
|  |  |  | 1. | | Не осуществляется настройка безопасности ОС на рабочих станциях | | | | | | | | | |  |  |  |  |
|  |  |  |  | пользователей. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | При покидании пользователем рабочего места не производится блокировка АРМ. | | | | | | | | | |  |  |  |  |
|  |  |  | 3. | | Для аутентификации используются слабые пароли, настройки парольной | | | | | | | | | |  |  |  |  |
|  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | |  |  |  |  |
|  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | |  |  |  |  |
|  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | |  |  |  |  |
|  |  |  |  | неуспешных попыток ввода пароля, не настроены параметры блокирования рабочей | | | | | | | | | | |  |  |  |  |
|  |  |  |  | станции после определенного периода неактивности. | | | | | | | |  |  |  |  |  |  |  |
|  | 3. Угрозы | типа |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | уязвимостей НДВ в системном | |  | средства ИСПДн - | |  | доступности | |  | вероятность | |  |
|  | «Отказ | в |  |  |  |  |  |  |
|  | обслуживании», в | |  |  |  |  | ПО |  |  | ОС | |  | ПДн | |  |  |  |  |
|  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |
|  | том | числе |  |  |  |  |  |
|  | 1. | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  | использование | |  |  |  |  |
|  | 2. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | известных |  |  |  |  |  |
|  |  |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 3. | | В ЛВС используются только коммутаторы и маршрутизаторы (хабы не | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | используются). | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 4. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  |  |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  | 4. Угрозы |  |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  |  | нарушитель | |  | уязвимостей, | вызванных |  | средства ИСПДн: | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного |  |  |  |  |  |  |  |
|  |  |  |  |  |  | наличием НДВ в системном ПО | |  | ОС | |  | ости, | |  |  |  |  |
|  | запуска |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | целостностии | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | приложений, в том | |  |  |  |  |  |  |  |  |  |  |  | доступности | |  |  |  |  |  |
|  |  | числе: | |  |  |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |  |
|  |  | - распространение | |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |  |
|  |  | файлов, | | 1. | | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |  |
|  |  | содержащих | | 2. | | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |  |
|  |  | несанкционирован | |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |  |
|  |  | ный исполняемый | |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |  |
|  |  | код; | | 3. | | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |  |

* переполнение обновление антивирусного ПО. Управление антивирусным ПО осуществляется

буферацентрализовано.

приложений-4.При осуществлении взаимодействия с сетью Интернет используются средства

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | серверов; | межсетевого экранирования. | | | |  |  |  |  |  |  |  |
|  |  | -использование | 5. | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | |  |  |  |
|  |  | возможностей |  |  |  |  |  |  |  |  |  |  |  |
|  |  | удаленного |  |  |  |  |  |  |  |  |  |  |  |
|  |  | управления |  |  |  |  |  |  |  |  |  |  |  |
|  |  | системой |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Угрозы 2-го типа |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 5. Угроза НСД с | Внутренний | | Доступ в | операционную | среду | Технические | | Нарушение | Средняя |  |  |
|  |  | нарушитель | | ИСПДн, | реализуемый | при | средства | ИСПДн | конфиденциальн | вероятность |  |  |
|  |  | применением |  |  |
|  |  |  |  | помощи | эксплуатации | НДВ | (АРМ |  | ости, |  |  |  |
|  |  | стандартных |  |  |  |  |  |  |
|  |  |  |  | (уязвимостей прикладного ПО), | | | пользователей, | | целостностии |  |  |  |
|  |  | функций |  |  |  |  |  |
|  |  |  |  | осуществляемый | | при | сервера |  | доступности |  |  |  |
|  |  | прикладного ПО |  |  |  |  |  |  |
|  |  |  |  | физическом доступе к ИСПДн | | | приложений/БД | | ПДн |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  | или | средствам | ввода | ИСПДн) |  |  |  |  |  |
|  |  |  |  |  | информации в ИСПДн | |  | Программные | |  |  |  |  |
|  |  |  |  |  |  |  |  | средства | ИСПДн: |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

ППО, СУБД

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института, ответственность за безопасность рабочих станций возложена на работников.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
2. При покидании пользователем рабочего места не производится блокировка АРМ.
3. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 6. Угроза | НСД с | Внутренний | Реализуется путем эксплуатации | Технические | Нарушение | Средняя |  |
| нарушитель | НДВвприкладномПО | средства ИСПДн: | конфиденциальн | вероятность |  |
| применением | |  |
| Внешний | (известных уязвимостей) | сервера | ости, |  |  |
| специально | |  |  |
| нарушитель |  | приложений/БД | целостностии |  |  |
| созданных | для |  |  |  |
|  |  |  |  | ИСПДн | доступности |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | этого программ | |  |  |  |  |  |  |  |  | Программные | |  | ПДн | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | средства ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | ППО, СУБД | |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
2. При покидании пользователем рабочего места не производится блокировка АРМ.
3. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Угрозы | типа | Внешний | Реализуется путем эксплуатации | Программные | Нарушение | Низкая |  |
| нарушитель | уязвимостей НДВ в прикладном | средства ИСПДн | доступности | вероятность |  |
| «Отказ | в |  |
| обслуживании», в | |  | ПО | ППО, СУБД | ПДн |  |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | |  |  |
| том | числе |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | использование | | | 1. | | Используется лицензионное ПО надежных производителей. | | | | | | |  |  |  |  |  |  |  |
|  | известных | | | 2. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | уязвимостей в ПО | | |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 3. | | В ЛВС используются только коммутаторы и маршрутизаторы (хабы не | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | используются). | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 4. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | Факторы, повышающие вероятность реализации угрозы: средства анализа | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | защищенности не используются. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | 8. Угрозы | | |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | уязвимостей, | вызванных |  | средства ИСПДн: | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного | | |  |  |  |  |  |  |
|  |  |  |  |  | наличием НДВ в | прикладном |  | ППО, СУБД | |  | ости, | |  |  |  |  |
|  | запуска | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ПО |  |  |  |  |  | целостностии | |  |  |  |  |
|  | приложений, в том | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | доступности | |  |  |  |  |
|  | числе: | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |
|  | - распространение | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |
|  | файлов, | | | 1. | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  | содержащих | | |  |  |  |  |
|  | 2. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  | несанкционирован | | |  |  |  |  |
|  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  | ный | исполняемый | |  |  |  |  |  |
|  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |
|  |  |  | 3. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |
| - | | переполнение | |  |  |  |  |
|  | буфера | | |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | |  |  |  |  |
|  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | приложений- | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 4. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | серверов; | | |  |  |  |  |
|  |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
| - | | использование | |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |
|  | возможностей | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | удаленного | | |  | Факторы, | повышающие | | | | вероятность | | | | реализации | | | угрозы: средства анализа | | | | |  |  |  |  |
|  | управления | | |  | защищенности не используются. | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | системой |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы 3-го типа | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 9. Угрозы | утечки | |  | Внешний |  |  | Перехват |  |  | акустической | | | |  | Технические | | |  | Нарушение | |  | Маловероятн | |  |
|  |  | нарушитель |  |  | (речевой) |  | информации | | | | с |  | средства обработки | | |  | конфиденциальн | |  | ая | |  |
|  | акустической | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  | использованием | | | аппаратуры, | | | |  | ПДн, | ВТСС, | |  | ости ПДн | |  | вероятность | |  |
|  | (речевой) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | регистрирующей акустические и | | | | | | |  | строительные | | |  |  |  |  |  |  |  |
|  | информации | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | виброакустические | | |  | волны, | | а |  | конструкции, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | также |  | электромагнитные | | | | |  | инженерно- | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | излучения, | | оптические | | | | и |  | технические | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электрические | | |  | сигналы, | | |  | коммуникации, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | модулированные | | |  |  |  |  |  | персонал ИСПДн | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информативным | | | акустическим | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | сигналом. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Перехват |  |  | акустической | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | (речевой) |  | информации | | | | с |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | использованием | | | специальных | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электронных | | устройств | | | съема | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | речевой информации | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | речевой (акустический) ввод/вывод персональных данных в данной ИСПДн не | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | предусмотрен. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 10. Угрозы | | |  | Внешний |  |  | Просмотр | ПДн | | с | помощью | | |  | Технические | | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель |  |  | оптических | |  |  |  |  |  |  | средства обработки | | |  | конфиденциальн | |  | вероятность | |  |
|  | утечки | видовой | |  |  |  |  |  | средств с | | |  |  |  |  |
|  | информации | | |  | Внутренний |  |  | (оптикоэлектронных) | | | |  | ПДн, | помещения, | |  | ости ПДн | |  |  |  |  |
|  |  | нарушитель |  |  | экранов | дисплеев | | | и | других | |  | персонал ИСПДн | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

средств отображения средств

вычислительной техники,

информационно-

вычислительных комплексов,

технических средств обработки

графической, видео и буквенно-

цифровой информации

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
2. Средства отображения информации в офисных помещениях защищены от визуального просмотра.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Внешний | Просмотр ПДн | | с помощью | | Технические | Нарушение | Низкая |
| нарушитель | специальных |  | электронных | | средства обработки | конфиденциальн | вероятность |
|  | устройств съема, внедренных в | | | | ПДн, помещения, | ости ПДн |  |
|  | служебных | помещениях | | или | персонал ИСПДн |  |  |
|  | скрытно |  | используемых | |  |  |  |
|  | физическими | лицами | | при |  |  |  |
|  | посещении | ими | служебных | |  |  |  |
|  | помещений |  |  |  |  |  |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | |  |
| доступ в помещения Института, где расположены рабочие станции пользователей, | | | | | | |  |
| ограничен и контролируется. В случае удаленного использования рабочих станций за | | | | | | |  |
| границами контролируемой зоны Института ответственность за безопасность рабочих | | | | | | |  |
| станций возложена на работников. | | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | |  |  |  | Объект |  |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11. | | Угрозы |  |  | Внешний | |  | Перехват | техническими | | |  | Инженерно- | |  |  |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | средствами | побочных | | (не |  | технические | |  |  |  | конфиденциальн | |  | вероятность | |  |
|  | утечки | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | связанных | с | прямым | |  | коммуникации | |  |  |  | ости ПДн | |  |  |  |  |
|  | информации | | по |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | |  | функциональным | | значением | |  | (цепи |  |  |  |  |  |  |  |  |  |  |
|  | каналам ПЭМИН | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | |  | элементов |  | ИСПДн) | |  | электропитания, | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информативных | |  |  |  | шины заземления и | | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | электромагнитных | | полей | и |  | т.д.) Института | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электрических |  | сигналов, | |  | ВТСС (средства | | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | возникающих | при | обработке | |  | системы | охранной | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | ПДн техническими | | средствами | |  | и | пожарной | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | ИСПДн |  |  |  |  | сигнализации | | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | т.д.) Института | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Линии | связи | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | передачи данных | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Технические | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | средства обработки | | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | ПДн | (рабочие | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | станции, | сервера и | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | т.д.) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | при обработке информации на АРМ пользователей, основную опасность при | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | реализации угрозы утечки по каналам ПЭМИН представляют утечки из-за наличия | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | электромагнитных излучений монитора. Ввиду большого числа рабочих станция и | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | другого оборудования выделение необходимой информации из общей среды | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | представляется маловероятным. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12. | | Угрозы |  |  | Внутренний | |  | Реализуются с | использованием | | |  | Программные | |  |  |  | Нарушение | |  | Средняя | |  |
|  |  | нарушитель | |  | отчуждаемых |  | носителей | |  | средства | ИСПДн: | | | конфиденциальн | | |  | вероятность | |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | модификации | | | |  | Внешний | |  | информации. | | Осуществляются | | | | | |  | базовая | система | |  | ости, |  |  |  |  |  |
|  | базовой | | системы | |  | нарушитель | |  | перехват |  | паролей | | |  |  | или |  | ввода-вывода | | |  | целостности | и |  | | |  |
|  | ввода/вывода | | | |  |  |  |  | идентификаторов, | | | модификация | | | | |  | (BIOS). |  |  |  | доступности |  |  |  |  |  |
|  | (BIOS), перехвата | | | |  |  |  |  | программного | |  | обеспечения | | | | |  | Технические | | |  | ПДн |  |  |  |  |  |
|  | управления | | | |  |  |  |  | базовой системы ввода-вывода | | | | | | | |  | средства ИСПДн | | |  |  |  |  |  |  |  |
|  | загрузкой, | |  |  |  |  |  |  | (BIOS), | перехват | | | управления | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | перехвата | | или | |  |  |  |  | загрузкой | с | целью | | изменения | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | подбора | | паролей | |  |  |  |  | необходимой | | технологической | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | или |  |  |  |  |  |  |  | информации | | для | | получения | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | идентификаторов, | | | |  |  |  |  | НСД в | операционную | | | | |  | среду |  |  |  |  |  |  |  |  |  |  |  |
|  | а |  | также | |  |  |  |  | ИСПДн |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | использование | | | |  | Применяемые защитные меры, | | | | | | снижающие вероятность угроз: доступ в помещения | | | | | | | | | | | |  | | |  |
|  | технологических | | | |  | Института, | | где расположены рабочие станции пользователей, ограничен | | | | | | | | | | | | | | | и |  | | |  |
|  | паролей BIOS | | | |  | контролируется. В случае удаленного использования рабочих станций за границами | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | контролируемой зоны Института, ответственность за безопасность рабочих станций | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | возложена на работников. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Факторы,повышающиевероятностьреализацииугрозы:аутентификация | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | пользователей при доступе к BIOS не осуществляется. | | | | | | | | | | | | |  |  |  |  |  |  |  |  |  |
| 13. | | Угроза НСД | | |  | Внутренний | |  | Доступ в | операционную | | | | | | среду |  | Программные | | |  | Нарушение |  |  | Высокая | |  |
|  | нарушитель | |  | ИСПДн | с | использованием | | | | | |  | средства | ИСПДн: | |  | конфиденциальн | | вероятность | | |  |
|  | с | применением | | |  |  |  |  |  |
|  | стандартных | | | |  | Внешний | |  | программных | | и | программно- | | | | |  | ОС, | СУБД, | |  | ости, |  |  |  |  |  |
|  |  | нарушитель | |  | аппаратных | |  |  |  |  | средств | |  | прикладные | | |  | целостности | и |  |  |  |  |
|  | функций | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  |  | ввода/вывода | | рабочих | | | станций | | |  | системы. |  |  |  | доступности |  |  |  |  |  |
|  | операционной | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | (серверов), входящих | | | | | в | состав | |  | Технические | | |  | ПДн |  |  |  |  |  |
|  | системы, | | СУБД, | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ИСПДн, | осуществляемый | | | | | | при |  | средства ИСПДн | | |  |  |  |  |  |  |  |
|  | прикладной | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | физическом доступе | | | | к |  | ИСПДн | |  |  |  |  |  |  |  |  |  |  |  |
|  | программы | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | или | средствам | | |  |  |  | ввода |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

информации в ИСПДн

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Пароли в открытом виде в ИСПДн не хранятся.
6. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
2. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.
3. Пользователи обладают правами локальных администраторов на своих рабочих станциях.
4. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 14. Угроза НСД | Внутренний | Реализуется путем эксплуатации | Технические | Нарушение | Высокая |  |
| нарушитель | вредоносного кода с целью | средства ИСПДн: | конфиденциальн | вероятность |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | с | применением | |  |  | Внешний | |  | получения | доступа | к |  | сервера | |  | ости, |  |  |  |  |  |  |
|  |  | специально | |  |  |  | нарушитель | |  | программным | средствам | |  | приложений/БД | |  | целостности | и | | | |  |  |
|  |  | созданных | | для |  |  |  |  |  | ИСПДн |  |  |  | ИСПДн | |  | доступности |  |  |  |  |  |  |
|  |  | этого программ | |  |  |  |  |  |  |  |  |  |  | Программные | |  | ПДн |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | средства ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | ППО, СУБД | |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.

Факторы, повышающие вероятность реализации угрозы:

1. Не осуществляется настройка безопасности ОС на рабочих станциях пользователей.
2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
3. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.
4. Пользователи обладают правами локальных администраторов на своих рабочих

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

станциях.

1. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Угроза | |  | Внутренний | | Копирование выгруженной | | из |  | Программные | |  | Нарушение | Высокая |  |
|  | нарушитель | | ИСПДн | информации | на |  | средства | ИСПДн: |  | конфиденциальн | вероятность |  |
| утечки |  |  |  |  |  |
|  |  | Внешний | | отчуждаемые носители | |  |  | ОС, | СУБД, |  | ости ПДн |  |  |
| информации путем | | |  |  |  |  |  |
| нарушитель | |  |  |  |  | прикладные | |  |  |  |  |
| преднамеренного | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | системы. |  |  |  |  |  |
| копирования | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | |  |  |
| доступных ПДн на | | |  |  |
| 1. | Доступ | в помещения Института, | |  | где расположены | | | рабочие станции | |  |  |
| неучтенные (в том | | |  |  |  |
| числе |  |  | пользователей, ограничен и контролируется. В случае удаленного использования | | | | | | | | | |  |  |
|  |  | рабочих станций за границами контролируемой зоны Института ответственность за | | | | | | | | | |  |  |
| отчуждаемые) | | |  |  |
| безопасность рабочих станций возложена на работников. | | | | | | |  |  |  |  |  |
| носители, а | | также |  |  |  |  |  |
| 2. | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | |  |  |
| печать неучтенных | | |  |  |
| копий | документов | | 3. | Идентификация и аутентификация пользователей при входе в ОС на рабочих | | | | | | | | |  |  |
| с | ПДн | на | станциях осуществляется по доменным учетным записям и паролям. | | | | | | | | | |  |  |
| Факторы, повышающие вероятность реализации угрозы: | | | | | | |  |  |  |  |  |
| принтерах | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Не осуществляется контроль портов ввода/вывода на АРМ пользователей.
2. Пользователи обладают правами локальных администраторов на своих рабочих станциях.
3. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.
4. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. Угроза | Внутренний | Доступ в | операционную среду | | Программные | Нарушение | Высокая |  |
| нарушитель | ИСПДн | с | использованием | средства ИСПДн: | конфиденциальн | вероятность |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | | |  |  | Источник | |  | Способ реализации |  |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | внедрения | |  |  |  | Внешний | |  | вредоносных | программ, |  |  | ОС, | СУБД, | |  | ости, |  |  |  |  |  |  |
|  | вредоносных | | |  |  | нарушитель | |  | загруженных с использованием | |  |  | прикладные | | |  | целостностии | | |  |  |  |  |
|  | программ | |  | с |  |  |  |  | съемных носителей |  |  |  | системы, |  |  |  | доступности | | |  |  |  |  |
|  | использованием | | | |  |  |  |  |  |  |  |  | технические | | |  | ПДн |  |  |  |  |  |  |
|  | съемных | |  |  |  |  |  |  |  |  |  |  | средства ИСПДн. | | |  |  |  |  |  |  |  |  |
|  | носителей, | | а также | |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | |  |  |  |  |
|  | в | связи | | с | 1. | | Доступ в помещения Института, | | | | где расположены | | | | | рабочие | | станции | |  |  |  |  |
|  | подключением | | |  |  | пользователей, ограничен и контролируется. В случае удаленного использования | | | | | | | | | | | | | |  |  |  |  |
|  | стороннего | |  |  |  | рабочих станций за границами контролируемой зоны Института ответственность за | | | | | | | | | | | | | |  |  |  |  |
|  | оборудования | | |  |  | безопасность рабочих станций возложена на работников. | | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  | (компьютеров, | | |  | 2. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | | |  |  |  |  |  |  |
|  | КПК, | смартфонов, | | | 3. | | Идентификация и аутентификация пользователей при входе в ОС на рабочих | | | | | | | | | | | | |  |  |  |  |
|  | телефонов, | |  |  |  | станциях осуществляется по доменным учетным записям и паролям. | | | | | | | | | | | |  |  |  |  |  |  |
|  | фотоаппаратов, | | |  | 4. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | |  |  |  |  |
|  | видеокамер, флэш- | | | | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | | | | | |  |  |  |  |
|  | дисков и иных | | | | централизовано. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | устройств, | | в | том |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  | числе | имеющих | | | 1. | | Не осуществляется контроль портов ввода/вывода на АРМ пользователей. | | | | | | | | | | | | |  |  |  |  |
|  | выход | |  | в | 2. | | Пользователи обладают правами локальных администраторов на своих рабочих | | | | | | | | | | | | |  |  |  |  |
|  | беспроводные сети | | | |  | станциях. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | связи) | |  |  | 3. | | Для аутентификации используются слабые пароли, настройки | | | | | | | | | | | парольной | |  |  |  |  |
|  |  |  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  | неуспешных попыток ввода пароля. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17. | | Угроза | |  |  | Внутренний | |  | Использование | программ- |  |  | Технические | | |  | Нарушение | | |  | Высокая | |  |
|  |  | нарушитель | |  | анализаторов | пакетов |  |  | средства | ИСПДн | |  | конфиденциальн | | |  | вероятность | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | «Анализа сетевого | |  |  | Внешний | |  | (снифферов) для перехвата ПДн | | |  | (каналы связи) | |  | ости: |  |  |  |  |  |  |  |
|  |  | трафика» | |  |  | нарушитель | |  | (ииной | конфиденциальной | |  |  |  |  | исследование | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | информации), а также для | | |  |  |  |  | характеристик | | | | | |  |  |
|  |  |  |  |  |  |  |  |  | перехвата | идентификаторов и | |  |  |  |  | сетевого |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | паролей удаленного доступа (к | | |  |  |  |  | трафика, |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | сетевым службам) | | |  |  |  |  | перехват |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | передаваемых | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, | в | том | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | числе |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | идентификаторо | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ви | паролей | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | пользователей | | |  | | |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
2. Обеспечивается разграничение доступа к кроссовому оборудованию.
3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
4. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
5. При обмене информацией между площадками Института, передаваемый трафик защищается при помощи технологии VPN.
6. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.

7. При использовании беспроводных сетей осуществляется

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | идентификация/аутентификация пользователей по доменным учетным записям с | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | Интернет. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 1. | | Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | не удалено с рабочих станций пользователей. | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | Пользователи обладают правами локальных администраторов на своих рабочих | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | станциях. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 3. | | Для аутентификации | | | | | используются | | слабые пароли, настройки | | | | | | | парольной | |  |  |  |  |
|  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | неуспешных попыток ввода пароля. | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 18. Угроза | |  | Внутренний | |  | Передача | | запросов | | сетевым | |  | Технические | | |  | Нарушение | | |  | Высокая | |  |
|  |  | нарушитель | |  | службам | | хостов ИСПДн | | | и |  | средства | ИСПДн | |  | конфиденциальн | | |  | вероятность | |  |
|  | сканирования сети | |  |  |  |  |  |  |
|  |  | Внешний | |  | анализ ответов на них с целью: | | | | |  |  | (каналы | связи), | |  | ости: | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | | - | | инвентаризации | | | сетевых | |  | программные | | |  | определение | | |  |  |  |  |
|  |  |  |  |  |  |  | ресурсов (поиск узлов сети, | | | | | |  | средства ИСПДн | | |  | протоколов, | | |  |  |  |  |
|  |  |  |  |  |  |  | определение их адресов, типов | | | | | |  |  |  |  |  | доступных | | |  |  |  |  |
|  |  |  |  |  |  |  | ОС); | |  |  |  |  |  |  |  |  |  | портов сетевых | | |  |  |  |  |
|  |  |  |  |  |  | - | | выявления активных | | | сетевых | |  |  |  |  |  | служб, | | |  |  |  |  |
|  |  |  |  |  |  |  | служб, используемых портов, | | | | | |  |  |  |  |  | идентификаторо | | |  |  |  |  |
|  |  |  |  |  |  |  | версий программ (уязвимых); | | | | |  |  |  |  |  |  | в | соединений, | |  |  |  |  |
|  |  |  |  |  |  |  | - выявления неиспользуемых, но | | | | | |  |  |  |  |  | активных | | |  |  |  |  |
|  |  |  |  |  |  |  | установленных | | | сетевых служб | | |  |  |  |  |  | сетевых | | |  |  |  |  |
|  |  |  |  |  |  |  | (уязвимых) | |  |  |  |  |  |  |  |  |  | сервисов, | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | идентификаторо | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

в и паролей

пользователей.

Нарушение

доступности:

возможен отказ в

обслуживании

сканируемых

сетевых

сервисов

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Обеспечивается разграничение доступа к кроссовому оборудованию.
2. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
4. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.

Факторы, повышающие вероятность реализации угрозы:

1. Не используется система обнаружения/предотвращения вторжений.
2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
3. Пользователи обладают правами локальных администраторов на своих рабочих станциях.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 19. Угроза | |  |  | Внутренний | |  | Перебор паролей (в том числе с | | | |  | Технические | | |  | Нарушение |  |  | Высокая | |  |  |
|  |  |  |  | нарушитель | |  | использованием | |  |  |  | средства | ИСПДн | |  | конфиденциальн вероятность | | | | |  |  |
|  |  | выявления паролей | |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Внешний | |  | специализированного | | | ПО), |  | (каналы | связи), | |  | ости, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | нарушитель | |  | установка |  | вредоносных | |  | программные | | |  | целостности | и | | | |  |  |
|  |  |  |  |  |  |  |  |  | программ | для | перехвата | |  | средства ИСПДн | | |  | доступности |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | паролей, | подмена | доверенного | |  |  |  |  |  | ПДн: |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | объекта | сети | (IP-spoofing), | |  |  |  |  |  | выполнение |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | перехват | пакетов | | (sniffing). |  |  |  |  |  | любого |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | Взлом перехваченных | | | в сети |  |  |  |  |  | действия, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | защищенных паролей (хэш) | | | |  |  |  |  |  | связанного | с | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | получением |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | несанкциониров | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | анного доступа |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
3. Аутентификационные данные пользователей передаются в защищенном виде.
4. Пароли хранятся в виде хэш-сумм.
5. Осуществляются идентификация и аутентификация пользователей при входе в ОС по доменным учетным записям и паролям.
6. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.
7. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | Интернет. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | | | | |  |  |  |  |  |  |  |
|  |  |  | 1. | | Не используется система обнаружения/предотвращения вторжений. | | | | | | | | | | | | |  |  |  |  |
|  |  |  | 2. | | Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | не удалено с рабочих станций пользователей. | | | | | | | | | | |  |  |  |  |  |  |  |
|  |  |  | 3. | | Пользователи обладают правами администратора на рабочих станциях. | | | | | | | | | | | | |  |  |  |  |
|  |  |  | 4. | | Для аутентификации | | | | используются слабые пароли, настройки парольной | | | | | | | | |  |  |  |  |
|  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | неуспешных попыток ввода пароля. | | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | 20. Угроза | |  | Внутренний | |  | Несанкционированное | | | |  |  | Технические | |  | Нарушение | |  | Средняя | |  |
|  |  | нарушитель | |  | использование | |  | протоколов | | средства ИСПДн | | |  | конфиденциальн | |  | вероятность | |  |
|  | навязывания | |  |  |  |  |  |  |
|  |  | Внешний | |  | маршрутизации | | | (RIP, | OSPF, |  |  |  |  | ости, | |  |  |  |  |
|  | ложного маршрута | |  |  |  | | |  |  |  |  |  |
|  |  | нарушитель | |  | LSP, | EIGRP) | и | управления | |  |  |  |  | целостностии | |  |  |  |  |
|  | сети | |  |  |  | | |  |  |  |  |  |
|  |  |  |  |  | сетью | (ICMP, | | SNMP) | для |  |  |  |  | доступности: | |  |  |  |  |
|  |  |  |  |  |  |  |  | | |  |  |  |  |  |
|  |  |  |  |  |  |  | внесения | | изменений | | в |  | | |  | несанкциониров | |  |  |  |  |
|  |  |  |  |  |  |  | маршрутно-адресные таблицы | | | | |  | | |  | анное изменение | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | маршрутно- | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | адресных | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, анализ и | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | модификация | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | передаваемых | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | навязывание | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ложных | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | сообщений | |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Обеспечивается разграничение доступа к кроссовому оборудованию.
   1. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.

Факторы, повышающие вероятность реализации угрозы:

1. Не используется система обнаружения/предотвращения вторжений.
2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
3. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 21. Угроза | Внутренний | Перехват поискового запроса в | Технические | Нарушение | Средняя |  |
| нарушитель | протоколах удаленного поиска | средства ИСПДн | конфиденциальн | вероятность |  |
| внедрения ложного |  |
| объекта сети | Внешний | (ARP, DNS, WINS) - в сетях со |  | ости, |  |  |
| нарушитель | стеком протоколов TCP/IP, и |  | целостностии |  |  |
|  |  |  |  |
|  |  | выдача на него ложного ответа, |  | доступности |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | использование | | которого |  | | |  | ПДн: перехват и | | | | |  |  |
|  |  |  |  |  |  |  |  |  | приводит | к | требуемому |  | | |  | просмотр |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | изменению | в | маршрутно- |  | | |  | трафика, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | адресных данных | |  |  |  |  |  | несанкциониров | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | анный доступ | к | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | сетевым |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ресурсам, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | навязывание |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ложной |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | информации |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.
   1. Обеспечивается разграничение доступа к кроссовому оборудованию.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть

Интернет.

Факторы, повышающие вероятность реализации угрозы:

1. Не используется система обнаружения/предотвращения вторжений.
   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
   2. Для аутентификации используются слабые пароли, настройки парольной

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  | Объект |  |  |  | Нарушаемые | | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ | | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  | неуспешных попыток ввода пароля. | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 22. | | Угрозы типа | |  | Внутренний | | - | | привлечение | | части | | ресурсов | |  | Технические | | |  | Нарушение | | |  |  | Средняя | |  |
|  | нарушитель | |  | ИСПДн на обработку | | | | | пакетов, | |  | средства | ИСПДн | |  | доступности | | | за | вероятность | | |  |
|  | «Отказ | | в |  |  |  |  |  |
|  | обслуживании», в | | |  | Внешний | |  | передаваемых | | |  |  |  |  |  | (каналы | связи), | |  | счет: |  |  |  |  |  |  |  |
|  |  | нарушитель | |  | злоумышленником | | | |  |  | со |  | программные | | | - | | снижения | | |  |  |  |  |
|  | том числе: | |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | снижением | | |  | пропускной | | |  | средства ИСПДн | | |  | пропускной | | |  |  |  |  |  |
| - | | частичное | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | способности | | | каналов | | связи, | |  |  |  |  |  | способности | | |  |  |  |  |  |
|  | использование | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | производительности | | | | | сетевых | |  |  |  |  |  | каналов | | связи, | |  |  |  |  |
|  | ресурсов; | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | устройств, | | |  | нарушением | | |  |  |  |  |  | производительно | | | |  |  |  |  |
| - | |  | полное |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | требований | | | к |  | времени | |  |  |  |  |  | сти | сетевых | | |  |  |  |  |
|  | исчерпание | |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | обработки запросов; | | | |  |  |  |  |  |  |  |  | устройств; | |  |  |  |  |  |  |
|  | ресурсов; | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | - | | исчерпание ресурсов ИСПДн | | | | | |  |  |  |  | - | | снижение | | |  |  |  |  |
| - | | нарушение | |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  | при | | обработке | |  | пакетов, | |  |  |  |  |  | производительно | | | |  |  |  |  |
|  | логической | |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | передаваемых | | |  |  |  |  |  |  |  |  |  | сти | серверных | | |  |  |  |  |
|  | связности | | между |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | злоумышленником (занятие всей | | | | | | |  |  |  |  |  | приложений; | | |  |  |  |  |  |
|  | техническими | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | полосы | | пропускания | | | каналов | |  |  |  |  |  | - невозможности | | | |  |  |  |  |
|  | средствами | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | связи, | | переполнение | | | очередей | |  |  |  |  |  | передачи | |  |  |  |  |  |  |
|  | ИСПДн; | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | запросов на обслуживание); | | | | | |  |  |  |  |  |  | сообщений | | из-за | |  |  |  |  |
| - | | использование | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  | - | | передача | | нарушителем | | | |  |  |  |  |  | отсутствия | |  |  |  |  |  |  |
|  | ошибок | | в |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | управляющих | | | сообщений | | | от |  |  |  |  |  | доступа к | | среде | |  |  |  |  |
|  | программах. | | |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | имени | | сетевых | | устройств, | | |  |  |  |  |  | передачи, отказ в | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  |  |  | приводящих | | | к | изменению | | |  |  |  |  |  | установлении | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | маршрутно-адресных | | | | | данных | |  |  |  |  |  | соединения; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | или | | идентификационной | | | | и |  |  |  |  |  | отказ |  |  | в |  | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | | |  |  |  | Объект |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | аутентификационной | | |  |  |  |  |  |  | предоставлении | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | информации; | |  |  |  |  |  |  |  | сервиса; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | - | | передача | пакетов | | с |  | | |  | - невозможности | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | нестандартными | |  | атрибутами | |  | | |  | передачи, | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | или | имеющих | | длину, | |  | | |  | сообщений | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | превышающую | | максимально | | |  | | |  | (получения | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | допустимый размер | | |  |  |  |  |  |  | услуг) | из-за | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | отсутствия | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | корректных | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | маршрутно- | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | адресных | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | - | | нарушения | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | работоспособнос | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ти | сетевых | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | устройств | | |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
   1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
   4. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник | |  | Способ реализации | | |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 6. | | При |  | использовании | | | беспроводных | | | | сетей | |  | осуществляется | |  |  |  |  |
|  |  |  |  |  | идентификация/аутентификация пользователей по доменным учетным записям с | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | Интернет. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 1. | | Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | не удалено с рабочих станций пользователей. | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 2. | | Не используется система обнаружения/предотвращения вторжений. | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | 3. | | Для аутентификации | | | | используются | | слабые пароли, настройки парольной | | | | | | | |  |  |  |  |
|  |  |  |  |  | политики не соответствуют лучшим международным практикам. В частности, длина | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | пароля недостаточна (6 символов), срок действия пароля не ограничен и не | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | осуществляется блокирование учетной записи после некоторого количества | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | неуспешных попыток ввода пароля. | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |
| 23. | | Угрозы | |  | Внешний | |  | Реализуется путем эксплуатации | | | | |  | Технические | | |  | Нарушение | |  | Высокая | |  |
|  | нарушитель | |  | уязвимостей, | |  | вызванных | |  | средства | ИСПДн | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного | | |  |  |  |  |  |  |  |
|  |  |  |  |  | некорректными | | | настройками | |  | (каналы | связи), | |  | ости, | |  |  |  |  |
|  | запуска | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | операционной | | системы, СУБД, | | | программные | | | |  | целостностии | |  |  |  |  |
|  | приложений, в том | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | сетевых | сервисов, | | прикладного | |  | средства ИСПДн | | |  | доступности | |  |  |  |  |
|  | числе: | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ПО |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |
|  | - распространение | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Использование | | | скрытых | |  |  |  |  |  |  |  |  |  |  |  |
|  | файлов, | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | компонентов | |  | ("троянских" | |  |  |  |  |  |  |  |  |  |  |  |
|  | содержащих | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | программ) | | либо | штатных | |  |  |  |  |  |  |  |  |  |  |  |
|  | несанкционирован | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | средств | управления | | | и |  |  |  |  |  |  |  |  |  |  |  |
|  | ный | исполняемый | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | администрирования | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | компьютерных сетей | | | |  |  |  |  |  |  |  |  |  |  |  |  |
| - | | переполнение | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | буфера | | | 1. | | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  |  | приложений- | | | 2. | | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  | серверов; | | |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  | - | | использование | |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  |  | возможностей | | | 3. | | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |
|  |  | удаленного | | |  |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | |  |  |  |  |
|  |  | управления | | |  |  | централизовано. | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  | системой | | | 4. | | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |

1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
2. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.
3. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.

Факторы, повышающие вероятность реализации угрозы:

1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
2. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Внешний | Реализуется путем эксплуатации | Программные | Нарушение | Низкая |
|  | нарушитель. | web-уязвимостей | средства ИСПДн | конфиденциальн | вероятность |
|  | Внутренний |  |  | ости, |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | |  |  |  |  |  |  |  |  |  |  |  | целостности | и |  | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | доступности |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ПДн |  |  |  |  |  |
|  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  | | |  |
|  |  |  | 1. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  | 3. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | межсетевого экранирования. | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 24. Угроза | |  | Внутренний | |  | Реализуется через почтовый или | | | | | |  | Программные |  |  | Нарушение |  |  | Высокая | |  |
|  |  | нарушитель | |  | файловый | обмен. | | | Запись кода | |  | средства ИСПДн |  |  | конфиденциальн | | вероятность | | |  |
|  | внедрения по сети | |  |  |  |  |  |  |
|  | вредоносных | |  |  |  |  | вредоносного ПО в код других | | | | | |  |  |  |  | ости, |  |  |  |  |  |
|  |  |  |  |  | программ | с | целью | | | получения |  |  |  |  | целостности | и |  |  |  |  |
|  | программ | |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | управления |  |  | при | | запуске |  |  |  |  | доступности |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | зараженных | | файлов, | | | создание |  |  |  |  | ПДн |  |  |  |  |  |
|  |  |  |  |  |  |  | файлов-двойников | | | |  | для |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | легального |  | ПО, | | копирование | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | кода вредоносной программы в | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | каталоги | для | | последующего | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | запуска пользователем | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  | | |  |
|  |  |  | 1. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  | 2. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | обновление | |  | антивирусного | | | ПО. | | Управление | | антивирусным | ПО осуществляется | | | |  | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

централизовано.

1. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.

Факторы, повышающие вероятность реализации угрозы:

1. Пользователи обладают правами локальных администраторов на своих рабочих станциях.
2. В ходе обследования получены данные о низком уровне компьютерной грамотности пользователей вообще и информационной безопасности в частности.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Внешний | Реализуется путем эксплуатации | | Программные | Нарушение | Средняя |
| нарушитель, | уязвимостей, | вызванных | средства ИСПДн | конфиденциальн | вероятность |
| Внутренний | некорректными | настройками |  | ости, |  |
| нарушитель | операционной | системы, СУБД |  | целостностии |  |
|  | или сетевых сервисов | |  | доступности |  |
|  |  |  |  | ПДн |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | |  |

1. Обеспечивается разграничение доступа пользователей к ИСПДн.
   1. На серверах рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
   2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
   3. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.

Факторы, повышающие вероятность реализации угрозы: не осуществляется настройка безопасности ОС на рабочих станциях пользователей.

Определение актуальности угроз безопасности ПДн

Результаты определения актуальности угроз безопасности ПДн, обрабатываемых в ИСПДн:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Вероятность |  |  |  |  |  | Коэффициент |  |  | Возможность |  |  |  |  |  |  |  |  |
|  | Класс угроз |  |  |  |  |  |  | Y2 |  |  | реализуемости |  |  |  |  | Опасность |  |  | Актуальность |  |  |
|  |  |  |  |  | реализации |  |  |  |  |  |  | реализации |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | угрозы Y |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы первого типа | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением стандартных | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | функций операционной системы | | | |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением специально | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | созданных для этого программ | | |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы типа «Отказ в обслуживании», в | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | том числе | использование | | известных |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы удаленного запуска приложений, | | | |  | Низкая | | 2 | |  | 0,35 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | в том числе: |  |  |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ распространение файлов, содержащих | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | несанкционированный | | исполняемый | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ переполнение буфера | | приложений- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | серверов; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ использование | | возможностей | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | удаленного управления системой. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы второго типа | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением стандартных | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | функций прикладного ПО | |  |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением специально | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | созданных для этого программ | | |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы типа «Отказ в обслуживании», в | | | |  | Низкая | | 2 | |  | 0,35 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | том числе | использование | | известных |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |
|  | | | | |  |  |  |  |  |  |
| Угрозы удаленного запуска приложений, | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| в том числе: | |  |  |  | вероятность |  |  |  |  |  |
| ­ распространение файлов, содержащих | | | | |  |  |  |  |  |  |
| несанкционированный | | | | исполняемый |  |  |  |  |  |  |
| код; |  |  |  |  |  |  |  |  |  |  |
| ­ переполнение | | буфера | | приложений- |  |  |  |  |  |  |
| серверов; | |  |  |  |  |  |  |  |  |  |
| ­ использование | |  |  | возможностей |  |  |  |  |  |  |
| удаленного управления системой. | | | | |  |  |  |  |  |  |
| Угрозы третьего типа | | |  |  |  |  |  |  |  |  |
| Угрозы утечки акустической (речевой) | | | | | Маловероятн | 0 | 0,25 | Низкая | Низкая | Неактуальная |
| информации | |  |  |  | ая угроза |  |  |  |  |  |
| Угрозы утечки видовой информации | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
|  |  |  |  |  | вероятность |  |  |  |  |  |
|  |  |  |  |  | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
|  |  |  |  |  | вероятность |  |  |  |  |  |
| Угрозы утечки информации по каналам | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| ПЭМИН | |  |  |  | вероятность |  |  |  |  |  |
| Угрозы | модификации | | базовой системы | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| ввода/вывода | | (BIOS), | | перехвата | вероятность |  |  |  |  |  |
| управления загрузкой, перехвата или | | | | |  |  |  |  |  |  |
| подбора паролей или идентификаторов, а | | | | |  |  |  |  |  |  |
| также | использование | | технологических | |  |  |  |  |  |  |
| паролей BIOS | |  |  |  |  |  |  |  |  |  |
| Угроза НСД с применением стандартных | | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |
| функций операционной системы, СУБД, | | | | | вероятность |  |  |  |  |  |
| прикладной программы | | |  |  |  |  |  |  |  |  |
| Угроза НСД с применением специально | | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
| созданных для этого программ | | |  | вероятность |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Угроза | утечки | информации | путем | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
| преднамеренного копирования доступных | | | | вероятность |  |  |  |  |  |  |  |
| ПДн на неучтенные (в том числе | | | |  |  |  |  |  |  |  |  |
| отчуждаемые) носители, а также печать | | | |  |  |  |  |  |  |  |  |
| неучтенных копий документов с ПДн на | | | |  |  |  |  |  |  |  |  |
| принтерах | |  |  |  |  |  |  |  |  |  |  |
| Угроза внедрения вредоносных программ | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
| с использованием съемных носителей, а | | | | вероятность |  |  |  |  |  |  |  |
| также в связи с подключением стороннего | | | |  |  |  |  |  |  |  |  |
| оборудования | | (компьютеров, | КПК, |  |  |  |  |  |  |  |  |
| смартфонов, телефонов, фотоаппаратов, | | | |  |  |  |  |  |  |  |  |
| видеокамер,флэш-дисковииных | | | |  |  |  |  |  |  |  |  |
| устройств, в том числе имеющих выход в | | | |  |  |  |  |  |  |  |  |
| беспроводные сети связи) | | |  |  |  |  |  |  |  |  |  |
| Угроза «Анализа сетевого трафика» | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза сканирования сети | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза выявления паролей | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза | навязывания ложного маршрута | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
| сети |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза внедрения ложного объекта сети | | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угрозы типа «Отказ в обслуживании», в | | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
| том числе: | |  |  | вероятность |  |  |  |  |  |  |  |

* частичное использование ресурсов;
* полное исчерпание ресурсов;

­ нарушение логической связности

между техническим средствами

ИСПДн;

* использование ошибок в программах.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Угрозы удаленного запуска приложений, | | | Высокая | 10 | 0,75 | Высокая | Низкая |  | Актуальная |  |  |
| в том числе: |  |  | вероятность |  |  |  |  |  |  |  |  |
| ­ распространение файлов, содержащих | | |  |  |  |  |  |  |  |  |  |
| Низкая | 2 | 0,35 | Средняя | Низкая |  | Неактуальная |  |  |
| несанкционированный | | исполняемый |  |  |  |
| вероятность |  |  |  |  |  |  |  |  |
| код; |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| ­ переполнение | буфера | приложений- |  |  |  |  |  |  |  |  |  |
| серверов; |  |  |  |  |  |  |  |  |  |  |  |
| ­ использование |  | возможностей |  |  |  |  |  |  |  |  |  |
| удаленного управления системой. | | |  |  |  |  |  |  |  |  |  |
| Угроза внедрения | по сети | вредоносных | Высокая | 10 | 0,75 | Высокая | Низкая |  | Актуальная |  |  |
| программ |  |  | вероятность |  |  |  |  |  |  |  |  |
|  |  |  | Средняя | 5 | 0,5 | Средняя | Низкая |  | Неактуальная |  |  |
|  |  |  | вероятность |  |  |  |  |  |  |  |  |