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 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

49

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Угрозы 2-го типа |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 3. 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4. 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
4. не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Угрозы 3-го типа | | | | | |  | |  | |  | |  | |  | |  | |  | |  | |  | | |  | | | |  | |  | |  | | |  | | | |  | | |  | |  | | | |  | |  | |  | | | |  | |
| Класс угроз | | | | |  |  | | Источник | | |  |  | | Способ реализации | | | | | | | |  | | | | | | |  | |  | | Объект | | | | |  | |  | |  | |  | Нарушаемые | | | |  | |  | | Вероятность | | | |
|  |  | | угроз | | |  |  | |  | | | | | | |  | |  | | воздействия | | | | | | |  | |  | |  | свойства ИБ | | | |  | |  | | реализации | | | |
| 5. | | | 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 | | | | | | |  |  | | |  | | | |  | | |  |  |  | | | | | | |  |  | | |
|  | |  |  |  | |  | | |  |  | |  | | |  |  |  | |  |  |  | | |  | | | |  | | |  |  |  | | | | | | |  |  | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. Угроза НСД | | | | | Внутренний | | | Реализуется путем эксплуатации | | | | | Технические | | | | | Нарушение | | | Высокая | | | | |  |
| нарушитель | | | вредоносного кода с целью | | | | | средства ИСПДн: | | | | | конфиденциальн | | | вероятность | | | | |  |
|  | | | | |  |
|  |  | 7. 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

64

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | | |  |  | Источник | |  | Способ реализации |  |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 8.Угроза внедрения | |  |  |  | Внешний | |  | Доступ в информационную среду ИСПДН при помощи вредоносных | программ, |  |  | ОС, | СУБД, | |  |  |  |  |  | Высокая |  |  |
|  | 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. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |