Модель угроз безопасности ПДн, обрабатываемых в ИСПДн

«Портал ДПО» и «distance.learning.ru»

4.4.1. 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 «Портал ДПО», «distance.learning.ru»

(коэффициент Y1).

* соответствии с заданными критериями оценки определяется уровень

исходной защищенности ИСПДн «Портал ДПО»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  | Уровень |  |  |
|  | Технические и эксплуатационные характеристики ИСПДн | | | | | | | |  |  |  | защищеннос |  |  |
|  |  |  |  | ти |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. По территориальному | | | | | локальная | ИСПДн, | | развернутая | | в |  | Высокая | |  |
| размещению | | |  |  | пределах одного здания | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 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 | | | | | |  |  |  |  |
| которые | |  |  |  | информации | |  |  |  |  |  | Высокий | |  |
| предоставляются | | | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| сторонним | | |  |  |  |  |  |  |  |  |  |  |  |  |

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

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Портал ДПО», 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 «Портал ДПО», «distance.learning.ru» Y1=5.

Описание угроз безопасности ПДн

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Класс угроз** | **Источник угроз** | | **Способ реализации** | | | | | | **Объект воздействия** | | **Нарушаемые свойства ИБ** | | | **Вероятность реализации** | | |
| Угрозы 1-го типа | | | | | | | | | | | | | | | | |
| 1. Угроза НСД с применением стандартных функций операционной системы | Внутренний нарушитель | | Доступ в операционную среду ИСПДн, реализуемый при помощи эксплуатации НДВ (уязвимостей системного ПО),осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | | | | | | Технические средства ИСПДн (АРМ  пользователей, сервера приложений/БД ИСПДн) Программные средства ИСПДн:  ОС | | Нарушение  конфиденциальности,  целостности и  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Доступ в помещения, где расположены сервера, ограничен и контролируется. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. Не осуществляется настройка безопасности ОС на серверах. 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. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 2. Угроза НСД с применением специально  созданных для  этого программ | Внутренний нарушитель Внешний нарушитель | | Реализуется путем эксплуатации НДВ в системном ПО (известных уязвимостей) | | | | | | Технические средства ИСПДн:  сервера приложений/БД ИСПДн  Программные средства ИСПДн:  ОС | | Нарушение  конфиденциальности,  целостности и доступности ПДн | | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. Не осуществляется настройка безопасности ОС на серверах. 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. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 3. Угрозы типа  «Отказ в обслуживании», в том числе  использование известных уязвимостей в ПО | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей НДВ в системном ПО | | | | | | Программные средства ИСПДн - ОС | | Нарушение  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   **Факторы,повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для:   Системного ПО,сервисов и служб,которые закрывают известные и новые уязвимости | | | | | | | | | | | | |
| 4. Угрозы удаленного  запуска  приложений, в том числе:  - распространение файлов, содержащих несанкционированный исполняемый код;  - переполнение буфера приложений серверов;  - использование возможностей удаленного управления системой | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей, вызванных  наличием НДВ в системном ПО | | | | | | Программные средства ИСПДн:  ОС | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов 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. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы,повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | | | |
| Угрозы 2-го типа | | | | | | | | | | | | | | | | |
| 5. Угроза НСД с применением стандартных функций прикладного ПО | | Внутренний нарушитель | | | | Доступ в операционную среду ИСПДн, реализуемый при помощи эксплуатации НДВ  (уязвимостей прикладного ПО), осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | | | | Технические средства ИСПДн (АРМ  пользователей, сервера приложений/БД ИСПДн) Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Средняя вероятность | |
|  | | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Доступ в помещения, где расположены сервера, ограничен и контролируется. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользовтелей к ИСПДн   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |  | |
| 6. Угроза НСД с применением  специально  созданных для  этого программ | Внутренний нарушитель Внешний нарушитель | | Реализуется путем эксплуатации  НДВ в прикладном ПО  (известных уязвимостей) | | | | | | Технические средства ИСПДн: сервера приложений/БД ИСПДн  Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Идентификация и аутентификация осуществляется по локальным учетным записям и паролям. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 7. Угрозы типа  «Отказ в обслуживании», в том числе  использование известных уязвимостей в ПО | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей НДВ в прикладном ПО | | | | | | Программные средства ИСПДн ППО, СУБД | | Нарушение  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. На части серверов устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Средства анализа защищенности не используются | | | | | | | | | | | | |
| 8. Угрозы удаленного  запуска  приложений, в том числе:  - распространение файлов, содержащих несанкционированный исполняемый код; - переполнение буфера приложений серверов;  - использование возможностей удаленного управления системой | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей, вызванных  наличием НДВ в прикладном ПО | | | | | | Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности  ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов 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. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.      1. средства анализа защищенности не используются | | | | | | | | | | | | |
| Угрозы 3-го типа | | | | | | | | | | | | | | | | |
| 9. Угрозы утечки акустической (речевой) информации | | Внешний нарушитель | | | Перехват акустической (речевой) информации с использованием аппаратуры, регистрирующей акустические и вибро-акустические волны, а также электромагнитные излучения, оптические и электрические сигналы, модулированные информативным акустическим сигналом.  Перехват акустической (речевой) информации с использованием специальных электронных устройств съема речевой  информации | | | Технические  средства обработки  ПДн, ВТСС,  строительные конструкции, инженерно-технические коммуникации, персонал ИСПДн | | | | | Нарушение конфиденциальности ПДн | | | Маловероятная вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: речевой (акустический) ввод/вывод информации в данной ИСПДн не предусмотрен. | | | | | | | | | | | | | |
| 10. Угрозы утечки видовой информации | | Внешний нарушитель Внутренний нарушитель | | Просмотр ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации | | | Технические средства обработки  ПДн, помещения, персонал ИСПДн | | | | | | Нарушение конфиденциальности ПДн | | | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Доступ в помещения, где расположены сервера, ограничен и контролируется.  2. Средства отображения информации в серверных помещениях защищены от визуального просмотра. | | | | | | | | | | | | | |
|  | | Внешний нарушитель | | | | Просмотр ПДн с помощью специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений | Технические средства обработки ПДн, помещения, персонал ИСПДн | | | | | | Нарушение конфиденциальности ПДн | | | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: доступ в помещения, где расположены сервера, ограничен и контролируется. | | | | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 11. Угрозы  утечки информации по каналам ПЭМИН | Внешний нарушитель | Перехват техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных  электромагнитных полей электрических сигналов, возникающих при обработке ПДн техническими средствами  ИСПДн | Инженерно-технические коммуникации (цепи электропитания, шины заземления и т.д.) Института  ВТСС (средства и системы охранной и пожарной сигнализации и  т.д.) Института  Линии связи и передачи данных Технические  средства обработки  ПДн (рабочие станции, сервера и  т.д.) | Нарушение конфиденциальности ПДн | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: при обработке информации, 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 модификации базовой системы ввода/вывода (BIOS), перехвата управления  загрузкой,  перехвата или подбора паролей или идентификаторов, а также использование технологических паролей BIOS | | Внутренний  нарушитель  Внешний  нарушитель | | Реализуются с использованием отчуждаемых носителей информации. Осуществляются перехват паролей или идентификаторов, модификация программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с целью изменения необходимой технологической информации для получения НСД в операционную среду ИСПДн | | Программные средства ИСПДн: базовая система ввода-вывода (BIOS).  Технические средства ИСПДн | | Нарушение  конфиденциальности,  целостности и  доступности  ПДн | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность угроз: доступ в помещения, где расположены сервера, ограничен и контролируется.  Факторы, повышающие вероятность реализации угрозы: аутентификация пользователей при доступе к BIOS не осуществляется. | | | | | | | |
| 13. Угроза НСД с применением стандартных функций  операционной системы, СУБД, прикладной программы | | Внутренний  нарушите ль  Внешний  нарушите  ль | | Доступ в операционную среду ИСПДн с использованием программных и программно-аппаратных средств ввода/вывода рабочих станций (серверов), входящих в состав ИСПДн, осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | | Программные средства ИСПДн: ОС, СУБД, прикладные системы. Технические средства ИСПДн | Нарушение  Конфиденциальности, целостности  доступности ПДн | и | | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Используется лицензионное ПО надежных производителей.  2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  3. Доступ в помещения, где расположены сервера, ограничен и контролируется.  4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям.  5. Пароли в открытом виде в ИСПДн не хранятся.  6. Обеспечивается разграничение доступа пользователей к ИСПДн.  7. Пользователи не обладают административными правами на серверах.  Факторы, повышающие вероятность реализации угрозы:  1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  2. Требования парольной политики не настроены и не контролируются. | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 14. Угроза НСД с применением  специально созданных  для этого программ | Внутренний  нарушитель | Реализуется путем эксплуатации вредоносного кода с целью получения доступа к программным средствам ИСПДн | Технические средства ИСПДн: сервера приложений/БД | Нарушение  конфиденциальности,  целостности и доступности ПДн | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы:   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 4. Требования парольной политики не настроены и не контролируются.   Пользователи обладают правами локальных администраторов на своих рабочих станциях. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 15. Угроза утечки информации путем преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать неучтенных копий документов с ПДн на принтерах | Внутренн ий  нарушите ль  Внешний нарушитель | Копирование выгруженной из  ИСПДн информации на  отчуждаемые носители | Программные средства ИСПДн:  ОС, СУБД, прикладные системы. | Нарушение конфиденциальн ости ПДн | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Доступ в помещения, где расположены сервера, ограничен и контролируется.  2. Обеспечивается разграничение доступа пользователей к ИСПДн.  3. Идентификация и аутентификация пользователей осуществляется по локальным учетным записям и паролям.  4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: требования парольной политики не настроены и не контролируются. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 16. Угроза внедрения  вредоносных  программ с  использованием съемных носителей, а также в связи с  подключением стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, флэшдисков и иных устройств, в том числе имеющих выход в беспроводные сети связи) | Внутренний  нарушитель  Внешний  нарушитель | Доступ в операционную среду ИСПДн с использованием вредоносных программ, загруженных с использованием съемных носителей | Программные средства ИСПДн: ОС, СУБД,  прикладные системы, технические средства ИСПДн. | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в помещения, где расположены сервера, ограничен и контролируется. 2. Обеспечивается разграничение доступа пользователей к ИСПДн. 3. Идентификация и аутентификация пользователей осуществляется по локальным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Требования парольной политики не настроены и не контролируются. 6. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 17. Угроза  «Анализа сетевого трафика» | Внутренний  нарушитель  Внешний  нарушитель | Использование программ-  анализаторов пакетов (снифферов) для перехвата ПДн (и иной конфиденциальной информации), а также для перехвата идентификаторов и паролей удаленного доступа (к сетевым службам) | Технические средства ИСПДн (каналы связи) | Нарушение конфиденциальности:  исследование характеристик сетевого трафика, перехват передаваемых  данных, в том числе идентификаторов и паролей пользователей | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в помещения, где расположены сервера, ограничен и контролируется. 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. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Доступ пользователей осуществляется по незащищенному протоколу http | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 18. Угроза сканирования сети | Внутренний  нарушитель  Внешний  нарушитель | Передача запросов сетевым службам хостов ИСПДн и анализ ответов на них с целью:   * инвентаризации сетевых ресурсов (поиск узлов сети, определение их адресов, типов ОС); * выявления активных сетевых служб, используемых портов, версий программ (уязвимых); * выявления неиспользуемых, но установленных сетевых служб   (уязвимых) | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение конфиденциальности:  определение протоколов, доступных портов сетевых служб, идентификаторов соединений, активных сетевых  сервисов,  идентификаторов и паролей пользователей. Нарушение доступности: возможен отказ в обслуживании сканируемых сетевых сервисов | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа к кроссовому оборудованию. 2. Доступ в помещения, где расположены сервера, ограничен и контролируется. 3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Не используется система обнаружения/предотвращения вторжений. 6. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов.   Пользователи обладают правами локальных администраторов на своих рабочих станциях. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 19. Угроза выявления паролей | Внутренн ий  нарушите ль  Внешний  нарушите  ль | Перебор паролей (в том числе с использованием  специализированного ПО), установка вредоносных программ для перехвата паролей, подмена доверенного объекта сети (IPspoofing), перехват пакетов (sniffing). Взлом перехваченных в сети защищенных паролей (хэш) | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение  конфиденциальн  ости,  целостности и доступности ПДн: выполнение любого  действия,  связанного с получением несанкциониров анного доступа | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 2. Пароли хранятся в виде хэш-сумм. 3. Осуществляются идентификация и аутентификация пользователей при входе в ОС по доменным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Не используется система обнаружения/предотвращения вторжений. 6. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 7. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 8. Требования парольной политики не настроены и не контролируются. 9. Пользователи обладают правами администратора на рабочих станциях.   Доступ пользователей осуществляется по незащищенному протоколу http. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 20. Угроза навязывания ложного маршрута  сети | Внутренний  нарушитель  Внешний  нарушитель | Несанкционированное использование протоколов маршрутизации (RIP, OSPF, LSP, EIGRP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы | Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и доступности: несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа к кроссовому оборудованию. 2. Доступ в помещения, где расположены сервера, ограничен и контролируется. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений.   Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 21. Угроза внедрения ложного объекта сети | Внутренний  нарушитель  Внешний  нарушитель | Перехват поискового запроса в протоколах удаленного поиска (ARP, DNS, WINS) - в сетях со стеком протоколов TCP/IP и выдача на него ложного ответа, использование которого приводит к требуемому изменению в  маршрутно-адресных данных | Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и доступности ПДн: перехват и просмотр трафика, несанкционированный доступ к  сетевым ресурсам, навязывание ложной информации | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в серверное помещение ограничен и контролируется. 2. Обеспечивается разграничение доступа к кроссовому оборудованию. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений.   Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 22. Угрозы типа  «Отказ в обслуживании», в том числе:   * частичное использование ресурсов; * полное исчерпание ресурсов; * нарушение логической связности между техническими   средствами ИСПДн;   * использование   ошибок в программах | Внутренний  нарушитель  Внешний  нарушитель | * привлечение части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов; * исчерпание ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание);   передача нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации;   * - передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение доступности за счет:  - снижения  пропускной способности каналов связи, производительности сетевых устройств; снижение производительности серверных приложений; - невозможности передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении  соединения;  отказ в предоставлении сервиса;   * невозможности передачи, сообщений (получения   услуг) из-за  отсутствия корректных маршрутно-адресных  данных;   * нарушения   работоспособности сетевых устройств | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).   На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Не используется система обнаружения/предотвращения вторжений. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 23. Угрозы удаленного запуска приложений, в том числе:   * распространение файлов, содержащих несанкционированный   исполняемый код;   * переполнение буфера приложений серверов; | Внешний  нарушитель | Реализуется путем эксплуатации уязвимостей, вызванных некорректными настройками операционной системы, СУБД, сетевых сервисов, прикладного ПО  Использование скрытых компонентов ("троянских" программ) либо штатных средств управления и администрирования компьютерных сетей | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Обеспечивается разграничение доступа пользователей к ИСПДн. 4. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.   Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Доступ пользователей осуществляется по незащищенному протоколу http. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Внешний нарушитель.  Внутренний  нарушитель | Реализуется путем эксплуатации web-уязвимостей | Программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая вероятность |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.   Факторы, повышающие вероятность реализации угрозы:   1. Информационные системы построены при помощи открытых платформ, при разработке не учитывались требования безопасного программирования. Системы защиты класса WAF (web application firewall) не применяются. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости Информационные системы построены при помощи открытых платформ, при разработке не учитывались требования безопасного программирования. Системы защиты класса WAF (web application firewall) не применяются. 4. Доступ пользователей осуществляется по незащищенному протоколу http.   Отсканированные документы, которые прикрепляют кандидаты в систему «mioo.ru», доступны по внешней ссылке без авторизации любому лицу, знающему ее. | | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 24. Угроза внедрения по сети вредоносных программ | Внутренний  нарушитель | Реализуется через почтовый или файловый обмен. Запись кода вредоносного ПО в код других программ с целью получения управления при запуске зараженных файлов, создание файлов-двойников для легального  ПО, копирование кода вредоносной программы в каталоги для последующего  запуска пользователем | Программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Факторы, повышающие вероятность реализации угрозы:  1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  3. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. | | | |
| Внешний нарушитель,  Внутренний  нарушитель | Реализуется путем эксплуатации уязвимостей, вызванных некорректными настройками операционной системы, СУБД или сетевых сервисов | Программные средства ИСПДн | Нарушение конфиденциальности,  целостности и  доступности ПДн | Высокая вероятность |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Факторы, повышающие вероятность реализации угрозы:   1. Не осуществляется настройка безопасности ОС на рабочих станциях пользователей и серверах. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется.   На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости | | | |