ПРИЛОЖЕНИЕ

к Положению о политике

информационной безопасности

администрации Суровикинского

муниципального района Волгоградской области

ВОЗМОЖНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ОПИСАНИЕ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N п/п | Название угрозы | Возможные источники угрозы | Используемые уязвимости | Вид активов, потенциально подверженных угрозе | Возможные последствия реализации угрозы |
| 1. | Осуществление несанкционированного доступа (ознакомления) с целевой информацией при ее обработке и хранении в ИС администрации района | пользователи ИС администрации района | недостатки механизмов разграничения доступа к целевой информации, связанные с возможностью предоставления доступа к целевой информации неуполномоченным на это лицам | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации |
| 2. | Осуществление несанкционированного копирования (хищения) информации, содержащей конфиденциальные сведения | пользователи ИС администрации района | недостатки механизмов безопасного взаимодействия автоматизированных рабочих мест (далее - АРМ) пользователей с серверами ИС | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации |
| 3. | Осуществление необнаруженной несанкционированной модификации (подмены) защищаемой информации | пользователи ИС администрации района | недостатки механизмов разграничения доступа к защищаемой информации и механизмов аудита, связанные с возможностью необнаруженной модификации (подмены) целевой информации неуполномоченными на это лицами | защищаемая информация | навязывание должностным лицам модифицированной (ложной) информации;  передача по запросам модифицированной (ложной) информации и нарушение режимов функционирования ИС |
| 4. | Осуществление необнаруженного несанкционированного блокирования (нарушение доступности) защищаемой информации | пользователи ИС администрации района;  другие лица, являющиеся внешними по отношению к ИС | недостатки механизмов безопасного администрирования сервисов, предоставляемых ИС, а также механизмов аудита, связанные с возможностью бесконтрольного блокирования доступности защищаемой информации | защищаемая информация | непредставление целевой информации заинтересованным лицам в отведенное время;  нарушение штатного режима функционирования ИС |
| 5. | Перехват защищаемой информации в каналах связи с использованием специально разработанных технических средств и ПО | пользователи ИС;  уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | недостатки механизмов защиты передаваемой информации, связанные с возможностью ее перехвата из каналов связи и последующего с ней ознакомления | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации, используемой в ИС;  несанкционированное ознакомление с принципами функционирования механизмов защиты в ИС, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС |
| 6. | Внедрение в ИС компьютерных вирусов | пользователи ИС;  уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | недостатки механизмов защиты информационных ресурсов ИС от компьютерных вирусов | программное обеспечение | нарушение режимов функционирования ИС;  реализация различного рода негативных информационных воздействий на целевую, технологическую информацию и программное обеспечение ИС |
| 7. | Осуществление необнаруженных несанкционированных информационных воздействий (направленных на "отказ в обслуживании" для сервисов, модификацию конфигурационных данных программно-аппаратных средств и т.п.) на программно-аппаратные элементы ИС | пользователи ИС администрации района; другие лица, являющиеся внешними по отношению к ИС | недостатки механизмов защиты программно-аппаратных элементов ИС от несанкционированных внешних воздействий | защищаемая информация, программное обеспечение | нарушение режимов функционирования ИС;  снижение уровня защищенности ИС; подготовка к последующим воздействиям и осуществление несанкционированного доступа к защищаемым информационным ресурсам |
| 8. | Осуществление несанкционированного доступа к информационным активам, основанного на использовании средств защиты информации, телекоммуникационного оборудования с уязвимостями и недокументированными возможностями, внесенными на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств | пользователи ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | наличие недекларированных возможностей, внесенных на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации; нарушение режимов функционирования |
| 9. | Осуществление несанкционированного доступа к защищаемой информации, основанного на восстановлении (в том числе фрагментарном) остаточной информации путем анализа выведенных из употребления, сданных в ремонт, на обслуживание, переданных для использования другим пользователям или для использования за пределами ИС носителей информации | пользователи ИС;  уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | недостатки механизмов гарантированного уничтожения защищаемой информации, связанные с возможностью ее последующего несанкционированного восстановления | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации |
| 10. | Внедрение в ИС вредоносного программного обеспечения | пользователи ИС;  уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | недостатки механизмов защиты информационных ресурсов ИС от вредоносного программного обеспечения | защищаемая информация, программное обеспечение | несанкционированное ознакомление и разглашение защищаемой информации;  создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС;  нарушение режимов функционирования ИС |
| 11. | Перехват разглашаемых сведений о защищаемой информации, ИС и ее компонентах | сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам;  обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) | недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью перехвата разглашаемой защищаемой информации | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации;  создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС |
| 12. | Хищение производственных отходов (распечаток, записей, списанных носителей) с целью последующего анализа и несанкционированного ознакомления с целевой и технологической информацией | сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам;  обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) | недостатки организационно-технических мер, обеспечивающих гарантированное уничтожение производственных отходов в ИС, связанные с возможностью их несанкционированного хищения и последующего использования для проведения аналитических исследований | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы |
| 13. | Осуществление несанкционированного визуального просмотра защищаемой информации, отображаемой на средствах отображения (экранах мониторов), а также несанкционированное ознакомление с распечатываемыми документами, содержащими защищаемую информацию | сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) | недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью несанкционированного визуального просмотра защищаемой информации на средствах отображения (экранах мониторов) | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы |
| 14. | Осуществление несанкционированного доступа к защищаемой информации в процессе ремонтных и регламентных работ | уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС | доступ лиц, имеющих право на техническое обслуживание, к техническим и программным средствам ИС в момент обработки с использованием этих средств защищаемой информации | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС;  нарушение режимов функционирования ИС |
| 15. | Осуществление несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам | сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам;  обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) | недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам | защищаемая информация | несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы |