Приложение 2

УТВЕРЖДЕНЫ
приказом департамента по
регулированию контрактной
системы Краснодарского края
от 25.06.2021 № 68

Требования к защите автоматизированных рабочих мест внешних пользователей региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд

1. Система защиты информации автоматизированных рабочих мест (далее – АРМ) внешних пользователей должна обеспечивать нейтрализацию следующих актуальных угроз безопасности информации (в соответствии с Частной моделью угроз):

Угроза отказа электропитания АРМ пользователей;

Угроза некорректной настройки программного обеспечения;

Угроза использования информации идентификации/аутентификации, заданной по умолчанию;

Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом);

Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей);

Угроза преодоления физической защиты;

Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию;

Угроза физического выведения из строя средств передачи информации;

Угроза хищения АРМ, обрабатывающих защищаемую информацию;

Угроза хищения средств передачи информации;

Угроза изменения компонентов системы (аппаратной конфигурации) АРМ;

Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

Угроза подбора пароля;

Угроза эксплуатации уязвимостей используемого программного обеспечения;

Угроза установки и использования устаревших и (или) уязвимых версий программного обеспечения;

Угроза (не)санкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию;

Угроза (не)санкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений;

Угроза внедрения вредоносного кода или данных на АРМ пользователей;

Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет;

Угроза получения сведений об информационной системе;

Угроза исследования работы приложения;

Угроза реализации атаки «человек посередине» при передаче информации в пределах контролируемой зоны;

Угроза реализации атаки «человек посередине» при передаче информации за пределы контролируемой зоны;

Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;

Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования;

Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика;

Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации;

Угроза нарушения функционирования технологических/информационн ых процессов вследствие некорректной работы средств защиты информации;

Угроза несанкционированного воздействия на средство защиты информации, его параметры настройки;

Угроза проникновения из смежных информационных систем с более низким уровнем защищенности;

Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники;

Угроза несанкционированного доступа к защищаемой памяти ядра процессора;

Угрозы, связанные с использованием методов социальной инженерии.

2. Система защиты информации АРМ внешних пользователей должна реализовывать следующие меры защиты информации в соответствии с требованиями методических документов, разработанных и утвержденных Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России):

ИАФ.1 – идентификация и аутентификация пользователей, являющихся работниками оператора;

ИАФ.3 – управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

ИАФ.4 – управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

ИАФ.5 – защита обратной связи при вводе аутентификационной информации;

УПД.1 – управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

УПД.2 – реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

УПД.3 – управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

УПД.4 – разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

УПД.5 – назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

УПД.6 – ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

УПД.10 – блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

УПД.11 – разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

ОПС.3 – установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

ЗНИ.1 – учет машинных носителей информации;

ЗНИ.2 – управление доступом к машинным носителям информации;

РСБ.1 – определение событий безопасности, подлежащих регистрации, и сроков их хранения;

РСБ.2 – определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

РСБ.3 – сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

РСБ.4 – реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

РСБ.5 – мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

РСБ.6 – генерирование временных меток и (или) синхронизация системного времени в информационной системе;

РСБ.7 – защита информации о событиях безопасности;

АВЗ.1 – реализация антивирусной защиты;

АВЗ.2 – обновление базы данных признаков вредоносных компьютерных программ (вирусов);

СОВ.1 – обнаружение вторжений;

СОВ.2 – обновление базы решающих правил;

АНЗ.1 – выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

АНЗ.2 – контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

АНЗ.3 – контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

АНЗ.4 – контроль состава технических средств, программного обеспечения и средств защиты информации;

АНЗ.5 – Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе;

ОЦЛ.1 – контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

ОЦЛ.3 – обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

ЗТС.2 – организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

ЗТС.3 – контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

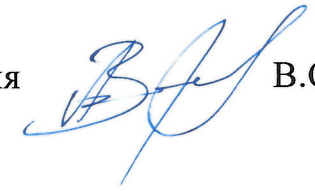
ЗТС.4 – размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

ЗИС.3 – обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

ЗИС.17 – разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

3. В случае наличия в составе локальной вычислительной сети (далее – ЛВС) пользовательского сегмента внешних пользователей региональной информационной системы Краснодарского края, используемой в сфере

закупок для обеспечения государственных и муниципальных нужд (далее – Система), АРМ, не входящих в состав Системы, такие АРМ должны дополнительно оснащаться сертифицированными ФСТЭК России средствами сетевой безопасности, реализующим функции межсетевого экранирования с целью обеспечения сегментирования ЛВС и функции средства обнаружения вторжений уровня хоста (реализующим меры СОВ.1, СОВ.2).

Начальник отдела
информационно-аналитического сопровождения  В.С. Лабунец