Приложение

УТВЕРЖДЕНО
приказом
АО «НПП «Исток» им. Шокина»
от 18.12.2025 № 03/2627

СТАНДАРТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОДРЯДНЫХ ОРГАНИЗАЦИЙ/ПОСТАВЩИКОВ УСЛУГ АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «ИСТОК» ИМЕНИ А.И. ШОКИНА»

Содержание

1. Общие положения

1.1. Стандарт информационной безопасности для подрядных организаций/поставщиков услуг акционерного общества «Научно-производственное предприятие «Исток» имени А.И. Шокина» (далее – Стандарт) устанавливает требования, необходимые для обеспечения информационной безопасности АО «НПП «Исток» им. Шокина» (далее – Общество) и предъявляемые к подрядным организациям/поставщикам услуг/третьим лицам (далее – Исполнитель), которые привлекаются к проведению пусконаладочных работ или имеют доступ к информационным активам Общества для выполнения работ в соответствии с заключенными договорами.

1.2. Целью стандарта является обеспечение непрерывности и безопасности бизнес-процессов Общества и минимизации вероятности реализации угроз безопасности информации со стороны Исполнителя.

1.3. Стандарт разработан на основании:

— Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

— приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

— ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

— ГОСТ Р ИСО/МЭК 27033-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей.».

— ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения»;

— ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства

обеспечения безопасности. Основы управления доступом».

1.4. Требования Стандарта в обязательном порядке включаются в договоры с Исполнителями, которые в рамках исполнения договоров привлекаются к пусконаладочным работам или которым в рамках исполнения договоров предоставляется доступ к информационной инфраструктуре Общества в той степени, в какой они применимы к формату предоставления услуг и (или) выполнения работ в рамках заключаемого договора.

1.5. Требования Стандарта доводятся Исполнителем до всех привлекаемых субподрядчиков, привлекаемых для исполнения таких договоров.

2. Термины и определения

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, предназначенный для автоматизации деятельности.

Аутентификация – действия по проверке подлинности пользователя или иного субъекта доступа, а также по проверке принадлежности пользователю или иному субъекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Виртуальная частная сеть (VPN) – защищенная сеть, создаваемая поверх общедоступной или иной сети, которая обеспечивает передачу информации с использованием средств криптографической защиты.

Временный пароль – условное слово или набор символов и знаков, использование которых ограничено по времени, для входа в систему после сброса индивидуального пароля.

Идентификатор – Признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию.

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

Информационная безопасность – состояние защищенности информационных ресурсов, при котором обеспечивается конфиденциальность целостность доступность, а также поддерживается устойчивость инфраструктуры к угрозам информационной безопасности.

Логин - имя (идентификатор) учётной записи пользователя в информационной системе.

Локальная вычислительная сеть (ЛВС) – совокупность аппаратных и программных средств, предназначенная для передачи и обработки информации на ограниченной территории в пределах одного здания или группы зданий.

Компрометация учетных данных – событие, в результате которого учетные данные легального субъекта доступа становятся или могут стать известными другому субъекту (другим субъектам) доступа.

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Метод аутентификации – реализуемое при аутентификации предопределенное сочетание факторов, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации.

Многофакторная аутентификация – аутентификация, при выполнении которой используется не менее двух различных по форме существования информации факторов аутентификации.

Несанкционированный доступ к информации (НСД) – доступ субъекта доступа к объекту доступа, нарушающий правила разграничения доступа.

ОИБ – отдел информационной безопасности Общества.

ОКиБ – отдел кибербезопасности Общества.

Пароль – секретная последовательность символов, известная только субъекту доступа и предназначенная для его аутентификации.

Съемный носитель информации (СНИ) – электронные носители информации и портативные устройства, подключаемые непосредственно к компьютеру, и имеющие возможность переноса информации.

Технические средства – физические компоненты, устройства и оборудование, обеспечивающие работу информационных и автоматизированных систем для выполнения определенных функций.

Удаленный доступ – процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ.

Фактор аутентификации – вид (форма) существования информации, используемой при идентификации и аутентификации.

3. Общие требования при предоставлении доступа Исполнителю к инфраструктуре Общества

3.1. Доступ к информационным активам Общества на основании заключенных договоров предоставляется в минимально необходимом для выполнения работ или

оказания услуг по договору объеме, а также при условии принятия Исполнителем обязательств по неразглашению и исключению неправомерного использования полученной в ходе выполнения работ или оказания услуг информации путем заключения соглашения о конфиденциальности между Обществом и всеми привлекаемыми для проведения работ представителями Исполнителя.

3.2. Удаленный доступ к информационным активам Общества предоставляется в соответствии с приказом от 01.10.2020 № 03/550 «Об утверждении и введении в действие безопасных схем подключения удаленных рабочих мест» и только после согласования такого доступа с ОИБ и ОКиБ.

3.3. При заключении договора Исполнитель должен определить представителя для взаимодействия по вопросам, связанным с обеспечением информационной безопасности.

3.4. Доступ к информационным активам Общества на основании договора предоставляется Исполнителям на определённый срок, не превышающий сроков выполнения работ по договору или действия договора, и прекращается по выполнении работ либо при прекращении действия договора.

3.5. Удаленный доступ для Исполнителя для выполнения работ/оказания услуг на значимых объектах критической информационной инфраструктуры Общества не предоставляется.

3.6. Общество оставляет за собой право ограничить или прекратить доступ к инфраструктуре в случае выявления нарушений Исполнителем требований Стандарта до их устранения.

4. Удаленное подключение Исполнителя к информационной инфраструктуре Общества

4.1. Удаленный доступ Исполнителя к информационным активам Общества осуществляется по защищенному каналу передачи данных (с использованием технологий VPN) с обязательной аутентификацией в инфраструктуре Общества при подключении.

4.2. Аутентификация в инфраструктуре Общества осуществляется по учетным данным, сформированным работниками Общества в соответствии с требованиями Положения об организации парольной защиты в АО «НПП «Исток» им. Шокина» и Политики разграничения и предоставления прав доступа в АО «НПП «Исток» им. Шокина».

4.3. Учетные данные для Исполнителя формируются на основании контактной информации о работниках Исполнителя, ответственных за выполнение работ/оказания услуг по договору: ФИО, номер телефона, адрес электронной почты, реквизиты договора.

4.4. Учетные данные, предоставляемые Исполнителю, закрепляются за конкретным работником и не должны использоваться совместно с другими работниками Исполнителя.

4.5. Пароли, используемые Исполнителем при таком подключении, подлежат изменению с периодичностью не реже, чем раз в 90 дней.

4.6. Работая в инфраструктуре Общества Исполнитель обязуется обеспечивать:

– организационные и технические меры по защите информации Общества от несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) информации в процессе обработки, передачи и хранения, а также по сохранению работоспособности технических средств Общества в соответствии с действующим законодательством Российской Федерации;

– конфиденциальность учетных данных для удаленного подключения, выданных Обществом;

– защищенность информации при доступе к инфраструктуре по защищенному каналу передачи данных во время выполнения работ;

– предотвращение несанкционированного копирования информации Общества с носителей информации и технических средств Исполнителя;

– контроль выполнения работ должностными лицами и работниками Исполнителя.

4.7. Для реализации вышеуказанных требований Исполнитель обязуется соблюдать требования по обеспечению информационной безопасности инфраструктуры Общества от угроз безопасности через свою инфраструктуру:

4.7.1. У Исполнителя должны быть утверждены политики, регламенты и процедуры в отношении обеспечения информационной безопасности с целью создания контролируемой среды для защиты информации от несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) информации в процессе обработки, передачи и хранения, а также по сохранению работоспособности технических средств.

4.7.2. Исполнитель в своей инфраструктуре должен реализовывать как минимум следующие требования к управлению доступом и парольной политике:

– регламентировать официальные процедуры управления доступом исходя из рабочих потребностей, обеспечив разделение полномочий по направлению запроса, утверждения и предоставления доступа;

– использовать стойкие пароли или многофакторную аутентификацию;

– использовать защищенную передачу временных паролей с обязательной сменой после первого входа;

– использовать пароли с истекающим сроком действия;

– не использовать учетные записи и пароли, установленные по умолчанию;

– не использовать совместные/общие учетные записи;

– обеспечивать незамедлительную блокировку учетной записи с последующим сбросом пароля при подозрении на компрометацию;

– блокировать учетные записи уволенных работников и неактивные учетные записи;

– обеспечивать блокировку сессии при неактивности;

– проводить периодическую проверку прав доступа всех пользователей;

– блокировать учетные записи после определенного количества неудачных попыток входа.

4.7.3. На всех сетевых интерфейсах Исполнителя должны быть установлены межсетевые экраны, обеспечивающие фильтрацию входящего и исходящего трафика и поддерживающие технологии IPS/IDS.

4.7.4. Для соблюдения требований конфиденциальности Исполнитель в отношении носителей информации должен:

– регламентировать процедуры учета, выдачи, использования и хранения съемных носителей информации (СНИ) с целью исключения несанкционированного доступа к ним;

– осуществлять контроль за использованием интерфейсов ввода/вывода информации на СНИ.

4.7.5. Исполнитель должен организовать физическую безопасность собственных технических средств, средств защиты информации и телекоммуникационного оборудования, исключающую несанкционированный физический доступ к таким средствам, а также обеспечивающий их защиту от внешних воздействий.

4.7.6. Исполнитель должен организовать управление конфигурацией информационной инфраструктуры и программного обеспечения, а также проведение периодической инвентаризации.

4.7.7. Исполнитель должен организовать непрерывную работу по управлению уязвимостями в прикладном и системном программном обеспечении своей инфраструктуры с целью их своевременного устранения.

4.7.8. На всех серверах и рабочих станциях (АРМ) Исполнителя должны использоваться средства антивирусной защиты с актуальными базами сигнатур, реализующие как минимум:

– регулярные периодические проверки на наличие вредоносного программного обеспечения;

– антивирусную проверку вложений в сообщениях электронной почты;

– обязательную антивирусную проверку съемных носителей информации при их подключении.

4.7.9. При работе в инфраструктуре Общества на технических средствах Исполнителя должна осуществляться регистрация событий безопасности. Регистрации подлежат как минимум следующие события:

– вход (выход), а также попытки входа субъектов доступа в операционную систему и загрузки (останова) операционной системы;

– подключение машинных носителей информации (СНИ) к техническим средствам Исполнителя и вывод информации на носители информации;

– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой информации Общества;

– попытки удаленного доступа к инфраструктуре Общества.

4.7.10. Исполнитель должен осуществлять мониторинг и реагирование на инциденты информационной безопасности и обязуется незамедлительно информировать Общество в случае:

– выявления в информационной инфраструктуре Общества или в своей инфраструктуре подозрительной активности, несанкционированного доступа, подозрения на заражение вредоносным программным обеспечением, нарушения работоспособности технических средств, иных признаков компьютерных инцидентов;

– компрометации учетных данных, выданных Обществом;

– выявлении факта несанкционированного доступа по удаленному каналу доступа, выделенному Исполнителю;

– выявлении факта несанкционированного копирования информации Общества.

5. Подключение технических средств Исполнителя к информационной инфраструктуре Общества

5.1. Подключение технических средств Исполнителя (ПК, ноутбук, СНИ) к информационной инфраструктуре Общества напрямую осуществляется при проведении работ по договору непосредственно на территории Общества после предоставления и согласования с Обществом перечня оборудования, используемого при выполнении работ, и контактной информации работников Исполнителя, ответственных за выполнение работ по договору.

5.2. При подключении АРМ (ПК, ноутбук) к информационной инфраструктуре Общества Исполнитель обязуется:

– не осуществлять несанкционированное подключение АРМ к сетевым розеткам и техническим средствам Общества;

– не подключать к техническим средствам Общества и к АРМ оборудование, не перечисленное в предоставленном Обществу перечне;

– использовать АРМ с лицензионным программным обеспечением и актуальной версией операционной системы, средствами антивирусной защиты с актуальными базами сигнатур;

– проводить антивирусную проверку на АРМ перед началом выполнения работ;

– обеспечивать защиту АРМ от несанкционированного доступа путем использования стойких паролей и настройке блокировки при неактивности;

– не допускать к работе на АРМ лиц, не являющихся ответственными за выполнение работ по договору и представителями Общества;

– не допускать несанкционированное копирование информации Общества на АРМ;

– блокировать АРМ при покидании рабочего места.

5.3. При использовании СНИ Исполнитель обязуется:

– обеспечивать сохранность СНИ, содержащих информацию Общества;

– не осуществлять несанкционированное подключение СНИ к техническим средствам Общества;

– проводить антивирусную проверку СНИ перед подключением к техническим средствам Общества;

– не хранить на подключаемых к техническим средствам Общества СНИ информацию, не имеющую отношения к выполнению работ по договору;

– не допускать несанкционированное копирование информации Общества на СНИ;

5.4. Исполнитель незамедлительно информирует Общество в случае:

– подозрения или выявления несанкционированного доступа к СНИ, АРМ или инфраструктуре Общества, компрометацию учетных данных АРМ;

– выявления в информационной инфраструктуре Общества подозрительной активности, подозрения на заражение вредоносным программным обеспечением, нарушения работоспособности технических средств, иных признаков компьютерных инцидентов;

– утраты носителей информации, содержащих информацию Общества;

– нарушения конфиденциальности информации Общества.