МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Ректор
_____ В.Д. Нечаев
«26» 12 2025 г.
№ 27-02-01-09/233

к приказу
от 26.12.2025 № 3200-п

РЕГЛАМЕНТ
взаимодействия ФГАОУ ВО «Севастопольский государственный университет» с подрядными организациями в целях обеспечения информационной безопасности автоматизированных информационных систем

Севастополь
2025

Содержание

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

1. Общие положения

1.1. Настоящий регламент определяет порядок взаимодействия ФГАОУ ВО «Севастопольский государственный университет» (далее – Университет) с подрядными организациями для обеспечения информационной безопасности автоматизированных информационных систем (АИС).

1.2. Регламент разработан в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и внутренней политикой Университета, а также письма Минобрауки России от 06.08.2025 №МН-19/995 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации». Цель — минимизация рисков, связанных с доступом третьих сторон к АИС, и защита конфиденциальной информации.

1.3. Регламент применяется ко всем этапам жизненного цикла АИС, включая проектирование, внедрение, эксплуатацию и сопровождение.

1.4. В настоящем Регламенте используются следующие понятия и определения:

АИС (автоматизированная информационная система) - это совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией.

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Двухфакторная аутентификация - метод проверки подлинности, при котором для входа в систему требуется подтверждение личности с использованием двух разных факторов.

Доступ — это возможность получения, просмотра, изменения, передачи или управления информацией в АИС. Он регулируется для предотвращения угроз, таких как несанкционированный вход, вредоносное ПО или внутренние инциденты.

Фишинг - вид интернет-мошенничества, при котором злоумышленники пытаются выманить у жертвы личную информацию под видом официального запроса.

Уязвимость - это слабое место в системе, которое может позволить злоумышленнику получить несанкционированный доступ, нарушить работу, украсть или изменить данные.

2. Цели и задачи

2.1. Обеспечение защиты информации в АИС от несанкционированного доступа, утечек и других угроз.

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

2.2. Установление четких требований к подрядным организациям в области информационной безопасности.

2.3. Регулирование взаимодействия между Университетом и подрядными организациями.

3. Обязанности сторон

3.1. **Субъект КИИ (Университет):**

- Определяет требования к информационной безопасности для подрядных организаций.
- Проводит оценку рисков и уязвимостей АИС.
- Обеспечивает контроль за выполнением требований информационной безопасности.

3.2. **Подрядные организации:**

- Соблюдают требования информационной безопасности, установленные Университетом.
- Проводят регулярные аудиты и тестирования на уязвимость своих систем и процессов.
- Уведомляют Университет о любых инцидентах, связанных с информационной безопасностью.

4. Требования к подрядным организация

4.1. Подрядная организация предоставляет Список работников, планирующих осуществлять удаленный доступ к информационной инфраструктуре организации по форме (приложение № 2 к акту - Список работников, планирующих осуществлять удалённый доступ к информационной инфраструктуре организации). В случае изменения состава указанных работников подрядная организация уведомляет о фактах таких изменений в течение 1 календарного дня в форме заявки об изменении состава работников подрядной организации (приложение № 3).

4.2. Подрядная организация предоставляет Политику информационной безопасности подрядной организации, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение инфраструктуры, План реагирования на компьютерные инциденты, а также Регламент действий работников в случае нештатных ситуаций, связанных с компьютерными инцидентами.

4.3. Подрядная организация предоставляет Университету Перечень контактов ответственных лиц по обеспечению информационной безопасности

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

в подрядной организации, включая каналы для оперативного взаимодействия (Приложение № 4 - Перечень контактов ответственных лиц по обеспечению информационной безопасности).

4.4. Удаленный доступ к информационной инфраструктуре Университета осуществляется при выполнении следующих мер подрядными организациями:

- наличие двухфакторная аутентификация;
- антивирусная защита автоматизированных рабочих мест и серверов;
- использование защищенного удаленного подключения с применением сертифицированных реестровых средств криптографической защиты информации;
- защита почтовых сервисов от фишинга;
- защищенный обмен файлами и информацией через файловое хранилище;
- обеспечение процесса управления уязвимостями;
- реализация парольной политики (длина пароля должна быть не менее 10 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов)). Пароли от учетной записи подрядной организации и учетной записи Университета должны отличаться.

4.5. Подрядная организация обеспечивает ведение записей всех действий пользователей при осуществлении удаленного подключения к инфраструктуре Университета. Срок хранения журнала событий не менее 1 года. В случае возникновения инцидента предоставлять указанный журнал событий Университету (приложение № 5 – пример).

4.6. Подрядным организациям запрещено использование программного обеспечения для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop).

4.7. Подрядные организации для доступа к информационной инфраструктуре Университета должны использовать средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

4.8. Подрядная организация уведомляет Университет при наступлении компьютерного инцидента в ее инфраструктуре (Приложение № 6).

4.9. Удаленный доступ предоставляется после подписания двустороннего Акта о фиксации перечня информации и информационных ресурсов для осуществления удаленного доступа (приложение № 1). Акт подписывается после проверки отделом защиты информации Центра развития и эксплуатации информационно-телекоммуникационной сети Дирекции информатизации и связи Университета выполнения подрядной организацией

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

всех требований.

5. Организация доступа и контроля ФГАОУ ВО «Севастопольский государственный университет»:

5.1. Разграничение доступа. Университет предоставляет подрядчику минимально необходимый доступ к АИС с выделением отдельных учётных записей и использованием принципа наименьших привилегий.

5.2. Университет проводить проверки и фиксирует местоположения удаленного доступа работников подрядной организации с указанием адреса (например, IP-адрес, страна) и формата такого подключения (например, локально или удаленно).

5.3. Университет ограничивает подключение к инфраструктуре Университета работников подрядной организации вне рабочего времени. В случае необходимости такие подключения должны быть согласованы с Университетом.

5.4 Университет обеспечивает (по возможности) включение информационной инфраструктуры подрядной организации в контур мониторинга информационной безопасности Университета (при ее наличии).

5.5. Университет проводит периодические проверки подрядной организации на предмет возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий.

5.6. При возникновении инцидента по информационной безопасности (неавторизованный вход, утечка данных и т.д. - со стороны подрядчика) Университет направляет заявку подрядной организации (Приложение № 7).

5.6. Университет осуществляет удаленный сетевой доступ с применением средств криптографической защиты информации, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам. Маршруты сетевого трафика не должны проходить по сторонним сетям в незашифрованном виде. Перечень IP-адресов, с которых может осуществляться подключение, должен контролироваться средствами межсетевого экранирования.

5.7. Учетные данные для доступа представителей подрядчика по договорам на разработку и/или сопровождение и/или внедрение программных продуктов в Университет формируются администраторами соответствующих платформ и направляются начальнику отдела защиты информации Центра развития и эксплуатации информационно-телекоммуникационной сети Дирекции информатизации и связи Университета или иному уполномоченному лицу, назначенное приказом ректора или (иным уполномоченным лицом) для персонального распространения, путем отправки работнику подрядчика на

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

корпоративный адрес, или на электронный адрес в домены *.ru, или в мессенджере MAX.

5.8. Проверку, настройку, конфигурирование и учет технических средств подрядчика для обеспечения доступа к соответствующей договору серверной платформе и/или информационной системе осуществляет лично начальник отдела защиты информации Центра развития и эксплуатации информационно-телекоммуникационной сети Дирекции информатизации и связи Университета или иное уполномоченное лицо, назначенное приказом ректора или (иным уполномоченным лицом).

6. Документация

6.1. Все взаимодействия между подрядными организациями и Университетом должны быть надлежащим образом задокументированы в следующих документах:

- Договорах с подрядными организациями.
-Протоколах заседаний и согласований.
- Отчетах об аудите и проверках.

7. Ответственность

7.1. В случае нарушения требований информационной безопасности стороны несут ответственность в соответствии с действующим законодательством и условиями договоров.

8. Заключительные положения

8.1. Настоящий Регламент вступает в силу с момента его утверждения приказом ректора Университета.

8.2. Внесение изменений и дополнений в настоящий Регламент осуществляется путём подготовки изменений (дополнений) в настоящий Регламент либо путём подготовки Регламента в новой редакции.

8.3. Принятие Регламента, изменений и дополнений к нему производится в соответствии с Инструкцией по делопроизводству Университета.

8.4. Настоящий Регламент подлежит регистрации и хранению в составе документов организационно-распорядительного характера номенклатуры дел отдела делопроизводства и архивного обеспечения Дирекции административных процессов. до замены его положением в новой редакции. Заверенная копия Регламента хранится в составе документов организационного характера Дирекции информатизации и связи.

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

Приложение № 1

АКТ № ____

о фиксации перечня информации и информационных ресурсов для осуществления удаленного доступа

г. Севастополь «___» _____ 20__ г.

ФГАОУ ВО «Севастопольский государственный университет» (далее - Университет), именуемый в дальнейшем «Заказчик», в лице _____ (должность, ФИО), с одной стороны, и _____ (наименование подрядной организации), именуемая в дальнейшем «Подрядчик», в лице _____ (должность, ФИО), с другой стороны, составили настоящий Акт о нижеследующем:

1. В рамках исполнения договора № ____ от «___» _____ 20__ г. Подрядчику предоставляется удаленный доступ к следующим информационным ресурсам Университета:

- Перечень информации: _____ (например, персональные данные студентов, научные материалы).

- Перечень информационных ресурсов: _____ (например, сервер базы данных _____).

2. Каналы связи, используемые для удаленного доступа:

- _____ (например, защищенный VPN-канал через провайдера "_____, IP-адреса: _____

- Требования к каналам: шифрование данных (AES-256), многофакторная аутентификация, мониторинг трафика.

3. Условия доступа:

- Доступ предоставляется только указанным работникам Подрядчика – Приложение № 2 к Акту (Список работников, планирующих осуществлять удалённый доступ к информационной инфраструктуре ФГАОУ ВО «Севастопольский государственный университет»).

- Срок доступа: с «___» _____ 20__ г. по «___» _____ 20__ г.

- Ограничения: доступ только в рабочее время Университета, без права копирования или передачи данных третьим лицам.

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

- Контроль: все действия логируются в системе мониторинга ИБ Университета.

4. Подрядчик обязуется соблюдать требования информационной безопасности Университета, включая неразглашение информации и немедленное уведомление о любых инцидентах.

5. Настоящий Акт составлен в двух экземплярах, имеющих равную юридическую силу.

Подписи:

Заказчик (Университет): _____ (подпись, печать)

Подрядчик: _____ (подпись, печать)

Приложение № 2 к Акту № ____
о фиксации перечня информации и
информационных ресурсов для
осуществления удаленного доступа

Список работников, планирующих осуществлять удалённый доступ к информационной инфраструктуре ФГАОУ ВО «Севастопольский государственный университет»

Подрядная организация: _____
Дата предоставления: «__» _____ 2025 г.

1. Общие сведения

Данный перечень включает работников подрядной организации, которым планируется предоставить удалённый доступ к информационным ресурсам и системам Университета в соответствии с условиями договора и Регламента взаимодействия ФГАОУ ВО «Севастопольский государственный университет» с подрядными организациями в целях обеспечения информационной безопасности автоматизированных информационных систем.

2. Список работников

№	ФИО работника	Должность	Контактный телефон	Служебный e-mail	Необходимые доступы	Обоснование необходимости	Планируемый срок доступа
1							
2							
3							

3. Ответственный за направление ИБ со стороны подрядчика

ФИО: _____
Должность: _____

Телефон: +7 (___) ___-__-__

E-mail: _____

4. Подтверждение достоверности сведений

Руководитель организации / Ответственный за работу с Университетом:

ФИО: _____

Должность: _____

Подпись: _____ Дата: «__» _____ 2025 г.

Приложение № 3

ЗАЯВКА

об изменении состава работников подрядной организации, планирующих осуществлять удалённый доступ к информационной инфраструктуре ФГАОУ ВО «Севастопольский государственный университет»

Подрядная организация: _____

Договор №: _____ от: _____

Объект выполнения работ:

_____

1. Выбывшие работники:

№	ФИО	Должность	Дата выбытия	Основание

2. Новые работники:

№	ФИО	Должность	Дата допуска

Просим внести соответствующие изменения для удалённого доступ к информационной инфраструктуре ФГАОУ ВО «Севастопольский государственный университет».

Дата: _____

Ответственное лицо: _____

Подпись: _____

Приложение № 4

Перечень контактов ответственных лиц по обеспечению информационной безопасности

Подрядная организация: _____

Дата предоставления: «__» _____ 2025 г.

1. Ответственные лица по информационной безопасности

1.1. Руководитель направления ИБ

ФИО: _____

Должность: _____

Телефон (раб.): +7 (___) ___-__-__

Телефон (моб.): +7 (___) ___-__-__

E-mail: _____

Часы доступности: _____

1.2. Специалист по реагированию на инциденты

ФИО: _____

Должность: _____

Телефон (моб.): +7 (___) ___-__-__

E-mail: _____

Часы доступности: 24/7 (по инцидентам ИБ)

1.3. Контакт для оперативной технической поддержки

ФИО: _____

Телефон (моб.): +7 (___) ___-__-__

E-mail: _____

Канал связи: Телефон, email, корпоративный мессенджер

2. Каналы для оперативного взаимодействия

Канал связи	Описание	Доступность
Для инцидентов ИБ: Email	Приём сообщений о выявленных угрозах, подозрительных активностях, нарушениях ИБ	24/7

Горячая линия ИБ: +7 (___) ___-__-__	Оперативная связь с дежурным специалистом	24/7
Техническая поддержка: E-mail:	Вопросы по доступам, системам, техническим сбоям	Пн–Пт, 09:00–18:00
Мессенджер MAX	Приём сообщений о выявленных угрозах, подозрительных активностях	По согласованию

Дата: _____

Ответственное лицо: _____

Подпись: _____

Приложение № 5

Пример журнала событий

Дата и время	Пользователь подрядчика	IP-адрес клиента	Событие	Результат	Комментарии / Подробности
2024-06-10 10:02:15	contractor_jdoe	203.0.113.45	Аутентификация в системе	Успешно	Использован ключ RSA, 2FA пройдена
2024-06-10 10:05:30	contractor_jdoe	203.0.113.45	Доступ к серверу базы данных	Успешно	Выполнен запрос SELECT, таблица users
2024-06-10 10:15:00	contractor_jdoe	203.0.113.45	Изменение конфигурации	Успешно	Обновлён конфигурационный файл nginx.conf
2024-06-10 10:45:20	contractor_jdoe	203.0.113.45	Завершение VPN-сессии	Успешно	Сессия ID: abc123 закрыта
2024-06-10 11:00:00	contractor_jdoe	203.0.113.45	Попытка доступа (неудача)	Неудачно	Ошибка аутентификации: неверный пароль

Приложение № 6

УВЕДОМЛЕНИЕ № ___
о компьютерном инциденте

Кому:_____
_____
(Должность, ФИО, название университета)

От:_____
_____
(Должность, ФИО, название подрядной организации) (Контактная информация)

Дата: _____

Тема: Уведомление о компьютерном инциденте в инфраструктуре (название организации)

Сообщаем, что (дата, время) в ИТ-инфраструктуре нашей организации произошел компьютерный инцидент, который потенциально может повлиять на взаимодействие с ФГАОУ ВО «Севастопольский государственный университет» (далее – Университет).

Краткое описание инцидента_____

Вид инцидента: _____

Описание события: о компьютерном инциденте
_____
_____

Затронутые системы/сервисы_____

Возможное влияние на Университет: _____

Принятые меры:_____

Локализация инцидента:_____

Устранение последствий:_____

Сроки восстановления:_____

Дополнительная информация:_____

Передано в компетентные органы: да/нет

Необходимые действия со стороны университета:
_____
_____