ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»

ПРИКАЗ

01.02.2022 Иркутск № 6

Об утверждении Политики
управления доступом

В целях соблюдения законодательства Российской Федерации в области защиты информации, руководствуясь Федеральным законом от 27.07.2006 №149 «Об информатизации, информационных технологиях и о защите информации»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику управления доступом в ФГБОУ ВО ИрГУПС (далее – Политика).
2. Начальнику общего отдела Курипко А.В. выставить Политику на внутреннем сайте Университета.
3. Редактору сайта Шикуевой В.Р. выставить Политику на официальный сайт Университета
4. Контроль за исполнением настоящего приказа возложить на проректора по цифровым технологиям Сачкова Д.И.

И.о. ректора А.П. Хоменко

СОГЛАСОВАНО
Проректор по цифровым технологиям Д.И. Сачков

Начальник управления информатизации Ю.Н. Шишкин

Начальник отдела информационной безопасности
и электронного документооборота Д.И. Майоренко

Приложение 1
к приказу от «01» 02 2022 г.
№ 6

Политика
управления доступом в ФГБОУ ВО ИрГУПС

1. Термины и сокращения

Авторизация	Определение и предоставление субъекту доступа соответствующих прав доступа.
Актив информационной безопасности (актив ИБ)	Всё, что имеет ценность и может потерять частично или полностью свойства информационной безопасности (конфиденциальность, доступность или целостность) при реализации угроз.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; проверка подлинности субъекта доступа.
Безопасность информации	Состояние защищённости информации, обрабатываемой средствами вычислительной техники, от внутренних или внешних угроз.
Владелец актива информационной безопасности	Определённая часть (структурное подразделение) организации, назначаемая руководителем организации ответственным за руководство изготовление, разработку, хранение, использование и безопасность актива. Термин «владелец» не означает наличие имущественных (и иных, не указанных в настоящей Политике) прав на актив.
Доступ к информации	Ознакомление с информацией, её обработка, в частности, копирование модификация или уничтожение информации.
Доступность информации	Свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.
Идентификатор доступа	Уникальный признак субъекта доступа.
Идентификация пользователей	Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Конфиденциальность информации	Свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.
Несанкционированный доступ	Доступ к активу, полученный в нарушении правил разграничения доступа.
Матрица доступа	Таблица, отображающая правила разграничения доступа;
Многофакторная (двухфакторная) аутентификация	Аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации;
Объект доступа	Компонент (единица) системы ФГБОУ ВО ИрГУПС или любой другой актив, доступ к которым регламентируется правилами разграничения доступа.

Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Рекомендация	Описание, поясняющее действия и способы их выполнения, необходимые для достижения целей, изложенных в Политике.
Роль доступа	Предопределённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.
Санкционированный доступ	Доступ к активу, полученный строго в рамках правил разграничения доступа.
СЗИ	Средства защиты информации.
СКЗИ	Средства криптографической защиты информации.
Средства обработки информации	Любая система обработки информации, услуга или инфраструктура, или их фактическое месторасположение.
Субъект доступа	Лицо или процесс, действия которого в отношении объектов доступа регламентируются правилами разграничения доступа.
Управление доступом	Ограничение, предоставление и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.
Целостность информации	Свойство безопасности информации, при котором отсутствует любое её изменение либо изменение субъектами доступа, имеющими на него право.

2. Общие положения

2.1. Настоящая Политика определяет цели и задачи в области обеспечения защиты информации, а также общие намерения и направления при управлении доступом к активам информационной безопасности информационных систем ФГБОУ ВО ИрГУПС.

2.2. Под активами информационной безопасности ФГБОУ ВО ИрГУПС понимаются информационные, программные и технические ресурсы ФГБОУ ВО ИрГУПС, которые могут потерять частично или полностью свойства информационной безопасности (конфиденциальность, доступность или целостность) при реализации угроз.

2.3. Настоящая Политика содержит:

– Политику управления доступом (Раздел 5);
– Политику идентификации и аутентификации пользователей (Раздел 6);
– Парольную Политику (Раздел 7);
– Удаленный доступ (Раздел 8);

2.4. В рамках настоящей Политики в качестве получателей прав доступа к активам информационной безопасности ФГБОУ ВО ИрГУПС (субъектов доступа, пользователей) рассматриваются:

– сотрудники ФГБОУ ВО ИрГУПС;
– обучающиеся ФГБОУ ВО ИрГУПС;
– привлекаемые в рамках Государственных контрактов или иных договоров специалисты и эксперты.

2.5. Настоящая Политика разработана на основании и в развитие:

– приказ ФГБОУ ВО ИрГУПС №547-1 «Об организации обработки персональных данных» от 22.09.2021;
– приказ ФГБОУ ВО ИрГУПС №295-1 «Об организации работы ИСПДн» от 20.05.2021;

– приказ ФГБОУ ВО ИрГУПС №134-1 «Об организации обработки персональных данных» от 01.09.2017 г.

2.6. Настоящая Политика создана и должна пересматриваться с учётом требований технологических процессов ФГБОУ ВО ИрГУПС и задач информационной безопасности.

3. Цели Политики управления доступом

Целями настоящей Политики являются:

– предотвращение несанкционированного доступа к активам информационной безопасности;

– предотвращение нарушений прав субъектов данных при обработке информации;

– недопущение деструктивного воздействия на технические средства обработки информации;

– недопущение деструктивного информационного воздействия на информацию.

4. Основные принципы управления доступом

4.1. Обоснованность доступа: должны существовать объективные причины, зафиксированные установленным порядком в соответствующих документах (соглашениях, регламентах, порядках, должностных инструкциях и др.), обуславливающие необходимость предоставления конкретному пользователю доступа к активу с определёнными полномочиями.

4.2. Разграничение прав доступа: субъектам доступа предоставляются только те права, которые необходимы ему для выполнения возложенных на него функциональных обязанностей.

4.3. Однозначность управления доступом: перечень активов и прав к ним, доступных пользователю, определяется набором типовых ролей (полномочий, шаблонов, профилей), описанных в эксплуатационной или иной документации на соответствующий актив информационной безопасности.

4.4. Документированность: управление (предоставление, изменение, блокировка, аннулирование) правами доступа к активам осуществляется исключительно на основании документа (заявки, иного обращения установленной формы на предоставление/изменение прав доступа), содержащей всю необходимую информацию для её однозначного и правильного выполнения.

4.5. Требования к мерам защиты информации, реализуемые при осуществлении доступа (требования к применяемым средствам защиты информации и организационным мероприятиям), должны соответствовать законодательству Российской Федерации, в том числе приказам Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17 и от 18.02.2013 г. № 21.

5. Правила управления доступом (Политика управления доступом)

5.1. Доступ к активам информационной безопасности предоставляется субъектам доступа (в том числе процессам), прошедшим этапы идентификации и аутентификации, в соответствии с Разделом 5 настоящей Политики. Исключение могут составлять действия, указанные в Перечне действий пользователей, разрешённых до прохождения ими процедур идентификации и аутентификации (Приложение №3).

5.2. Доступ к информации, относящейся к информации ограниченного распространения и информации ограниченного доступа, а также к активам, являющимся

средствами обработки информации такой классификации, допускается только для авторизованных субъектов доступа.

5.3. Необходимость авторизации доступа может быть определена владельцем и в отношении общедоступной информации и активов, являющихся средствами обработки информации указанной классификации. Данная необходимость должна быть определена в отношении активов в случае необходимости обеспечения целостности и доступности информации.

5.4. Настоящая Политика предусматривает следующие стандартные категории учётных записей (пользователей):

5.4.1. Непривилегированные учётные записи – по умолчанию для всех пользователей (субъектов доступа) ФГБОУ ВО ИрГУПС, которым не делегированы права привилегированных учётных записей.

5.4.2. Привилегированные учётные записи – для администраторов ФГБОУ ВО ИрГУПС и системных компонент:

– учётные записи системных администраторов – для пользователей, уполномоченных на выполнение действий по управлению (администрированию) инфраструктурой системы;

– учётные записи администраторов учётных записей (доступа) – для пользователей, уполномоченных на выполнение действий по управлению учётными записями и их правами в системах ФГБОУ ВО ИрГУПС;

– учётные записи администраторов безопасности - для пользователей, уполномоченных на выполнение действий по управлению средствами защиты информации;

– технологические (сервисные) учётные записи – для общесистемных компонент ФГБОУ ВО ИрГУПС.

5.5. Должно быть обеспечено разграничение между отдельными должностными лицами следующих полномочий:

– по обработке информации (пользователей);

– по администрированию актива ИБ (системные администраторы);

– по управлению системой защиты информации (администратор безопасности);

– по контролю (мониторингу) за обеспечением уровня защищённости информации;

– по обеспечению функционирования систем ФГБОУ ВО ИрГУПС.

5.6. Администратором, имеющим права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам и осуществляющим контроль за использованием переданных полномочий (Супервизором) в системах ФГБОУ ВО ИрГУПС является структурное подразделение УИ ФГБОУ ВО ИрГУПС, в полномочия которого входит организация и координация процессов управления информационной безопасностью.

5.7. Процессы предоставления доступа к активам информационной безопасности требующим авторизации субъектов доступа осуществляются с учётом разделения следующих полномочий:

– по запросу доступа;

– по авторизации доступа;

– по администрированию доступа.

5.8. Запрос доступа:

5.8.1. В отношении сотрудников ФГБОУ ВО ИрГУПС и работников подведомственных ФГБОУ ВО ИрГУПС организаций:

– для сотрудников должностью ниже заместителя начальника отдела – запрос доступа осуществляется начальником соответствующего отдела;

– для сотрудников с должностью заместитель начальника отдела и выше – запрос доступа осуществляется пользователем самостоятельно.

5.8.2. В отношении привлекаемых в рамках Государственных контрактов или иных договоров специалистов и экспертов запрос доступа осуществляется руководителем (уполномоченном лицом) организации, с которой непосредственно заключён Государственный контракт или договор.

5.8.3. В отношении компонента ИТ-инфраструктуры (процесса) запрос доступа осуществляется начальником структурного подразделения, являющегося владельцем актива информационной безопасности, к которому относится данный компонент.

5.9. Авторизация (подтверждение) доступа:

5.9.1. В отношении сотрудников ФГБОУ ВО ИрГУПС подтверждение доступа осуществляется совместно с:

– начальником структурного подразделения ФГБОУ ВО ИрГУПС к которому относится пользователь;

– начальником структурного подразделения ФГБОУ ВО ИрГУПС, в функции которого входит организация обеспечения выполнения нормативно-правовых документов по защите конфиденциальных сведений и персональных данных;

– начальником структурного подразделения ФГБОУ ВО ИрГУПС, являющимся владельцем актива (объекта доступа).

5.9.2. В отношении сотрудников филиалов ФГБОУ ВО ИрГУПС и работников подведомственных ФГБОУ ВО ИрГУПС организаций подтверждение доступа осуществляется совместно с:

– начальником структурного подразделения, в функции которого входит организация обеспечения выполнения нормативно-правовых документов по защите конфиденциальных сведений и персональных данных (в случае, если доступ запрашивается для пользователя одной организации к активу, относящемуся к другой организации, то авторизация доступа осуществляется начальниками соответствующих структурных подразделений в обеих организациях);

– начальником структурного подразделения, являющимся владельцем актива (объекта доступа);

– руководителем или заместителем руководителя организации, к которой относится пользователь.

5.9.3. В отношении привлекаемых в рамках Государственных контрактов или иных договоров специалистов и экспертов подтверждение доступа осуществляется совместно с:

– руководителем или уполномоченным лицом ФГБОУ ВО ИрГУПС или подведомственной ФГБОУ ВО ИрГУПС организации, заключившей соответствующий Государственный контракт (договор);

– начальником структурного подразделения, являющимся владельцем актива (объекта доступа);

– начальником структурного подразделения ФГБОУ ВО ИрГУПС или подведомственной ФГБОУ ВО ИрГУПС организации, в функции которого входит организация обеспечения выполнения нормативно-правовых документов по защите конфиденциальных сведений и персональных данных.

5.10. Администрирование доступа осуществляется пользователями ФГБОУ ВО ИрГУПС, уполномоченными на выполнение действий по управлению правами доступа к соответствующему активу (администраторы доступа).

5.11. Возможности администратора доступа администрировать собственные права доступа должны быть ограничены, в случае наличия такой технической возможности.

5.12. Запрос, авторизация и администрирование доступа осуществляются при условии заверения всеми ответственными лицами указанных действий личной подписью или квалифицированной электронной подписью.

5.13. Запрос и авторизация доступа могут быть оформлены как заявка, матрица доступа (допускается использование должностей и категорий пользователей вместо конкретных идентификаторов пользователей) или как иной документ при условии соблюдения принципов документированности. Допускается объединение учётных записей в группу пользователей.

5.14. Права доступа в отношении пользователей, у которых изменились должностные обязанности (переведённых на другую должность) или уволившихся, должны быть немедленно пересмотрены (отменены – в случае увольнения) администраторами доступа.

5.15. Права доступа в отношении привилегированных учётных записей должны регистрироваться администраторами доступа в соответствующих журналах и пересматриваться не менее двух раз в три месяца.

5.16. Должна быть обеспечена блокировка попыток несанкционированной загрузки нештатной среды (операционной системы) на активах ИБ, а также контроль целостности системного программного обеспечения и аппаратных компонент активов.

5.17. В случае неактивности пользователя при доступе к активу более 1 (одного) часа в рамках одного сеанса (в случае технической возможности для реализации), данный сеанс доступа должен быть заблокирован.

6. Правила управления учётными записями пользователей (Политика идентификации и аутентификации)

6.1. При идентификации пользователей должны использоваться уникальные идентификаторы, позволяющие отследить действия конкретных пользователей в конкретный момент времени (повторное использование одного идентификатора различными субъектами доступа должно быть исключено).

6.2. Использование общих учётных записей (учётных записей, которыми пользуется несколько пользователей) должно быть минимизировано и обосновываться особенностью выполнения технологических процессов и технической реализации актива. Учёт использования общих учётных записей конкретным пользователем должен выполняться за счёт реализации организационных мер (ведение журналов и пр.).

6.3. Аутентификация пользователей в системах ФГБОУ ВО ИрГУПС допускается:

– с использованием пароля, соответствующего Разделу 6 настоящей Политики;

– с использованием средств криптографической защиты информации и усиленной электронной подписи с применением сертификата ключа проверки электронной подписи;

– исключительно для доступа к общедоступной информации и активам, являющимся средствами обработки информации указанной классификации, допускается по согласованию с владельцем использование для аутентификации иной информации в электронном виде (например, в виде файла или ссылки в электронном сообщении);

– с использованием сертифицированных по требованиям ИБ электронных идентификаторов;

– с одновременным использованием нескольких вышеперечисленных способов (многофакторная аутентификация);

– по служебному удостоверению или документу, удостоверяющему личность (паспорт Российской Федерации).

6.4. Процедуры регистрации и блокировки учётных записей пользователей (и других пользовательских идентификаторов) должны быть формально учтены. В организации должен быть назначен ответственный за создание, присвоение и блокировку идентификаторов, а также за временное хранение, выдачу и инициализацию аутентификационной информации.

6.5. Соответствующими администраторами учётных записей должна проводиться периодическая (не менее двух раз в три месяца) проверка и блокирование избыточных пользовательских идентификаторов (учётных записей). Под избыточными пользовательскими

идентификаторами понимаются неиспользуемые более 45 дней, либо задублированные (при использовании в одной системе учётных записей нескольких идентификаторов, связанных с одним субъектом доступа).

6.6. Пользователи систем ФГБОУ ВО ИрГУПС при получении аутентификационной информации в обязательном порядке должны под роспись ознакомиться с настоящей политикой. При этом особое внимание пользователя необходимо обратить на обязанности пользователя (Приложение № 2).

6.7. Число разрешённых неудачных попыток аутентификации должно быть ограничено:

– для учётных записей пользователей – не более 3 в час;

– для привилегированных учётных записей – не более 3 в сутки.

После превышения указанного количества, устройство с которого осуществлялись попытки аутентификации должно быть заблокировано (при наличии технической возможности).

6.8. Попытки аутентификации в системах ФГБОУ ВО ИрГУПС должны записываться и храниться.

6.9. Процедура регистрации (создания идентификационной информации) в системе должна быть спроектирована так, чтобы свести к минимуму возможность несанкционированного доступа.

6.10. Необходимо, чтобы процедура начала сеанса раскрывала минимум информации о системе, во избежание оказания какой-либо ненужной помощи неавторизованному пользователю.

6.11. При вводе паролей в информационной системе, они не должны отображаться на экране.

6.12. Многократное использование одного идентификатора для доступа к одному активу должно быть ограничено.

6.13. При аутентификации пароли (и иная аутентификационная информация) не должны передаваться в открытом виде по сети.

6.14. В случае компрометации аутентификационной информации администраторами учётных записей должны быть приняты все меры по блокированию действий соответствующих учётных записей до проведения процедур по замене аутентификационной информации. По факту компрометации аутентификационной информации должны быть проведены мероприятия по выявлению причин компрометации и её последствий.

6.15. Для идентификации и аутентификации в системах ФГБОУ ВО ИрГУПС рекомендуется использовать единый сервис Active Directory.

6.16. В ИТ-инфраструктуре до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств обработки информации).

6.17. Идентификация устройств осуществляется по логическим именам устройств (доменным именам).

6.18. Аутентификация устройств обеспечивается с использованием протоколов аутентификации.

6.19. В системах ФГБОУ ВО ИрГУПС рекомендуется осуществлять идентификацию и аутентификацию объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа с использованием свидетельств подлинности информации.

7. Управление паролями пользователей (Парольная Политика)

7.1. Выдача паролей пользователю осуществляется исключительно при условии ознакомления пользователя под роспись с инструкцией по соблюдению требований информационной безопасности (Приложение № 2).

7.2. Должностные лица (администраторы учётных записей), ответственные за хранение, выдачу, инициализацию и блокировку паролей в организациях должны быть назначены.

7.3. Создание (смена) паролей может:

– осуществляться самостоятельно пользователем - предпочтительный вариант;

– осуществляться администратором учётных записей – в случае особенности технологического процесса, в том числе при использовании общих учётных записей.

7.4. В случае самостоятельной смены пользователем личных паролей, администратором учётных записей первоначально или повторно (в случае утери) предоставляется временный пароль, который подлежит немедленной принудительной замене пользователем после его первого использования для доступа.

7.5. Регламентами и порядками доступа к активам должны быть предусмотрены меры проверки личности пользователя, прежде чем ему будет предоставлен новый, заменяющий или временный пароль.

7.6. В случае управления паролями администратором учётных записей, администратором обеспечивается запись новых и замещающих паролей на парольной карте и их безопасное хранение в запечатанном виде на всё время использования пароля.

7.7. Пароли следует выдавать пользователям безопасным способом (обеспечивающим их конфиденциальность).

7.8. Пароли должны быть уникальны для каждого пользователя, не должны быть легко угадываемыми. Пароли должны формироваться с учётом следующих требований (для непривилегированных учётных записей):

– не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

– иметь длину не менее 8 знаков;

– содержать знаки трех из четырех перечисленных ниже категорий: латинские заглавные буквы (от A до Z), латинские строчные буквы (от a до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например, ! $, #, %).

7.9. Для привилегированных учётных записей должны соблюдаться следующие требования:

– минимальная длина паролей – 12 символов;

– содержание в пароле буквенных символов латинского алфавита – да;

– наличие не менее одного цифрового символа – да;

– содержание в пароле букв верхнего и нижнего регистра – да;

– содержание в пароле специальных символов (@,#,$,%,^) – да;

– минимальное отличие от предыдущего пароля – 3 символа.

7.10. Пароли непривилегированных учётных записей должны меняться не реже 1-го раза в 90 календарных дней; привилегированных учётных записей - не реже 1-го раза в 90 календарных дней.

7.11. Пользователи должны подтверждать получение паролей.

7.12. Хранение (и иная обработка) паролей в системах ФГБОУ ВО ИрГУПС должно производиться только в защищённой форме (с использованием СКЗИ – в электронной форме, и применением организационных мер – в иных случаях).

7.13. Пароли поставщика (разработчика/изготовителя), установленные по умолчанию, должны быть изменены после инсталляции в системах ФГБОУ ВО ИрГУПС лицом, осуществившем указанную инсталляцию, после чего на парольной карте переданы соответствующему администратору учётных записей.

7.14. Пользователи обязаны обеспечить конфиденциальность паролей, в том числе избегать запись паролей (например, на бумаге, в файле программного обеспечения или карманных устройствах), если не может быть обеспечено безопасное хранение и способ хранения не утверждён.

7.15. Пользователи обязаны сообщать администратору доступа о всех признаках возможной компрометации пароля.

7.16. Запрещается использование одного и того же пароля для работы в системах ФГБОУ ВО ИрГУПС и для личных целей (для доступа к личной электронной почте, для доступа к социальным сетям, личным аккаунтам в интернет-магазинах и прочее).

8. Удалённый доступ пользователей

8.1. Удалённый доступ пользователей к активам информационной безопасности, опубликованным в сети общего пользования Интернет, возможен исключительно для активов, к котором запрещён пользовательский внутренний доступ (из пределов систем ФГБОУ ВО ИрГУПС), и только в отношении активов, не требующих авторизации.

8.2. В случае необходимости предоставления удалённого доступа к активам, требующим авторизации, или активам, к которым одновременно осуществляется доступ пользователей из пределов информационной системы, должны выполняться следующие требования:

– на вычислительной технике должны быть реализованы необходимые меры защиты информации;

– удалённый доступ должен осуществляться исключительно по защищённым с использованием сертифицированного СКЗИ каналам связи;

– должна использоваться многофакторная (двухфакторная) аутентификация;

– перечень IP-адресов в сети Интернет, с которого предоставляется доступ к активам, должен быть ограничен.

8.3. При удалённом доступе пользователь обязан обеспечить необходимую защиту места дистанционной работы в отношении, например, хищения оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации или неправильного использования оборудования.

8.4. Виды работ, которые могут быть осуществлены удалённо, время работы, классификацию информации, к которой разрешён доступ сотруднику в дистанционном режиме, должны утверждаться начальниками подразделений с согласованием начальника управления информатизации.

Приложение 1
к Политике Управления доступом ФГБОУ ВО ИрГУПС
утверждённой приказом ФГБОУ ВО ИрГУПС
от «01» 02 2022 г.
№ 6

Рекомендации по определению владельца актива информационной безопасности

В общем случае владельцем актива определяется часть организации, ответственная за использование указанного актива. В отношении конкретных активов определение владельца рекомендуется осуществлять в соответствии с таблицей:

№	Актив ИБ	Определение владельца
1.	Серверные комплексы	Структурное подразделение, в обязанности которого входит обеспечение функционирования серверных комплексов. Или владельцы информационного ресурса, размещаемого на данном серверном комплексе.
2.	Рабочие станции, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных	Структурное подразделение, в пользование которого выдано оборудование.
3.	Активное и пассивное коммуникационное оборудование, система управления, мониторинга и обслуживания сетевой инфраструктуры	Структурное подразделение в обязанности которого входит обеспечение функционирования телекоммуникационных сетей в организации.
4.	Общесистемное программное обеспечение (операционные системы, системы управления базами данных)	Структурное подразделение в обязанности которого входит обеспечение функционирования общесистемного программного обеспечения или структурное подразделение, являющееся владельцем оборудования, на котором функционирует общесистемное ПО.
5.	Средства защиты информации	Структурное подразделение, в обязанности которого входит обеспечение информационной безопасности.
6.	Средства обеспечения жизнедеятельности объектов	Структурное подразделение, в обязанности которого входит обеспечение работоспособности соответствующего средства.
7.	Информация	В случае разработки (создания) указанной информации в организации, проводящей учёт активов – структурное подразделение, разработавшее указанную информацию. В случае поступления указанной информации из вне – определяется руководителем (заместителем руководителя) организации.

Приложение 2
к Политике Управления доступом ФГБОУ ВО ИрГУПС
утверждённой приказом ФГБОУ ВО ИрГУПС
от «01» 02 2022 г.
№ 6

Инструкция
пользователя при работе с активами информационной безопасности в системах ФГБОУ ВО ИрГУПС

1. Целью настоящего документа является обеспечение уверенности в том, что сотрудники ФГБОУ ВО ИрГУПС и подведомственных организаций, а также подрядчики (исполнители государственных контрактов) осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, что снижает риск человеческого фактора.
2. Пользователь обязан ознакомиться с соответствующей эксплуатационной документацией перед использованием актива, понимать свои обязанности при работе с активами и не использовать активы для целей, не соответствующих должностным обязанностям.
3. При использовании активов информационной безопасности пользователи должны обеспечивать сохранность аутентификационной информации, в том числе:
   - сохранять конфиденциальность паролей и закрытой ключевой информации;
   - избегать записи паролей, если не может быть обеспечено его и безопасное хранение и способ хранения не утверждён;
   - изменять пароли и сообщать об этом администратору информационной безопасности всякий раз, когда появляется любой признак возможной компрометации системы или пароля;
   - изменять временные пароли при первом начале сеанса;
   - не включать пароли ни в какой автоматизированный процесс начала сеанса, например, с использованием хранимых макрокоманд или функциональных клавиш;
   - не использовать коллективно индивидуальные пользовательские пароли;
   - не использовать один и тот же пароль для работы в системах ФГБОУ ВО ИрГУПС и для личных целей.
4. Пользователь несёт исключительную личную ответственность за все действия, осуществлённые с использованием его идентификатора (имени учётной записи или др.) и аутентификационной информацией.
5. Все пользователи при работе с активами информационной безопасности должны обеспечивать возможные процедуры по обеспечению безопасности, в том числе:
   - завершать активные сеансы по окончании работы, если отсутствует соответствующий механизм блокировки, например, защищённая паролем экранная заставка;
   - завершить сеанс на виртуальной инфраструктуре, серверах и офисных персональных компьютерах, когда работа завершена (т.е. не только выключить экран персонального компьютера или терминал);
   - обеспечивать безопасность персональных компьютеров или терминалов от несанкционированного использования с помощью блокировки клавиатуры или эквивалентных средств контроля, например, доступа по паролю, когда оборудование не используется.
6. Необходимо обеспечить Политику «чистого стола» в отношении бумажных документов и носителей данных, а также Политику «чистого экрана» в отношении средств обработки информации. Политика «чистого стола» и «чистого экрана» должна учитывать классификацию информации, законодательные и договорные требования, а также

соответствующие риски. В рамках соблюдения политик «чистого стола» и «чистого экрана» необходимо обеспечить выполнение следующих рекомендаций:

– носители (бумажные или электронные), содержащие информацию ограниченного доступа или ограниченного распространения, а также иной критической информации, когда они не используются, следует убирать и запирать (лучше всего, в несгораемый сейф или шкаф), особенно, когда помещение пустует;

– компьютеры, когда их оставляют без присмотра, следует выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем, носителем ключевой информации или аналогичным механизмом аутентификации пользователя, а также необходимо применять кодовые замки, пароли или другие меры и средства контроля и управления в то время, когда эти устройства не используются;

– необходимо обеспечить защиту пунктов приёма/отправки корреспонденции, а также автоматических факсимильных аппаратов

– документы, содержащие информацию ограниченного доступа или ограниченного распространения, а также иную критическую информацию, необходимо немедленно изымать из принтеров.

Приложение 3
к Политике Управления доступом ФГБОУ ВО ИрГУПС
утверждённой приказом ФГБОУ ВО ИрГУПС
от «01» 02 2022 г.
№ 6

Перечень действий пользователей, разрешённых до прохождения ими процедур идентификации и аутентификация

№	Наименование действия
1	Доступ к общедоступной информации и иным общедоступным ресурсам (в том числе сетевым ресурсам, файловым хранилищам и прочее)
2	Доступ к веб-сайтам, порталам, содержащим открытую информацию (в том числе Интернет-порталу ФГБОУ ВО ИрГУПС)
3	Доступ к системам информационно-правового обеспечения.
4	Действия привилегированных пользователей (администраторов), направленные на восстановление работоспособности системы и её отдельных компонентов
5	Действия привилегированных пользователей (администраторов), направленные на восстановление доступности информации в системах ФГБОУ ВО ИрГУПС