УТВЕРЖДЕНА
приказом *Об утверждении политики информационной безопасности ПетрГУ*
от «28» декабря 2020 г. № 734

Политика информационной безопасности в ПетрГУ

1. Общие положения

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается Ректором Федерального государственного бюджетного образовательное учреждение высшего образования «Петрозаводский государственный университет» (ПетрГУ) и определяет мероприятия, процедуры и правила по защите информации в информационных системах персональных данных (ИСПДн) ПетрГУ.

1.2. Положения настоящей Политики распространяются на все информационные системы персональных данных ПетрГУ.

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей ИСПДН ПетрГУ (далее - Пользователи), а также для администраторов безопасности информации и администраторов ИСПДН ПетрГУ (далее - Администраторы).

1.4. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.5. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

2. Правила и процедуры идентификации и аутентификации пользователей ИСПДн ПетрГУ, политика разграничения доступа к ресурсам ИСПДн ПетрГУ

2.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ПетрГУ, допущенному к работе с ИСПДн ПетрГУ присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИСПДн ПетрГУ.

2.2. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИСПДн ПетрГУ запрещено.

2.3. Администратор ИСПДн перед созданием учетной записи пользователя ИСПДн ПетрГУ осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности у начальника структурного подразделения пользователя. При создании учетной записи пользователя ИСПДн ПетрГУ Администратор ИСПД сообщает об этом Администратору безопасности ИСПДн для актуализации списка сотрудников, допущенных к обработке персональных данных в ИСПДн ПетрГУ.

2.4. Создание учетных записей пользователей ИСПДн для лиц, не являющихся сотрудниками ПетрГУ запрещено.

2.5. Начальник структурного подразделения пользователя незамедлительно оповещает Администратора ИСПДн, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

2.6. В качестве модели разграничения доступа к ресурсам ИСПДн ПетрГУ выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ИСПДн ПетрГУ.

2.7. Пользователям запрещены любые действия в ИСПДн до прохождения процедуры идентификации и аутентификации в системе.

2.8. В ИСПДн ПетрГУ установлено ограничение количества неуспешных попыток входа в ИСПДн (десять попыток), а также обеспечено блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток доступа к ИСПДн.

2.9. В ИСПДн ПетрГУ обеспечивается блокирование сеанса доступа пользователя после 60 минут его бездействия (неактивности) в ИСПДн или по запросу пользователя. Блокирование сеанса доступа пользователя в ИСПДн ПетрГУ сохраняется до прохождения им повторной идентификации и аутентификации.

2.10. Организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн ПетрГУ регламентируются Инструкцией по организации парольной защиты.

3. Правила и процедуры контроля установки обновлений программного обеспечения

3.1. С целью противодействия эксплуатации известных уязвимостей, в ПетрГУ устанавливаются правила и процедуры контроля установки обновлений системного и прикладного ПО.

3.2. В ПетрГУ обновление прикладного, системного программного обеспечения и средств защиты информации осуществляется Администратором ИСПДн.

3.3. Обновление микропрошивок и программного обеспечения BIOS производится только при поступлении информации о критичных уязвимостях в таком ПО, применяемом в ПетрГУ.

4. Правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации

4.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ИСПДн ПетрГУ фиксируется в техническом паспорте на ИСПДн. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

4.2. Администратор ИСПДн осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

4.3. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор ИСПДн принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5. Правила и процедуры выявления, анализа и устранения уязвимостей

5.1. В ПетрГУ в качестве средства выявления уязвимостей используется сканер уязвимостей OpenVAS.

5.2. Сотрудники отдела информационной безопасности не реже одного раза в месяц проводят полное сканирование системы на выявление уязвимостей.

5.3. Сотрудники отдела информационной безопасности изучают отчеты по результатам сканирования и принимают решение о немедленном устранении выявленных уязвимостей.

5.4. В случае невозможности оперативного устранения критичной уязвимости, начальник отдела информационной безопасности уведомляет об этом директора РЦНИТ и Ответственного за организацию обработки персональных данных в ПетрГУ.

6. Правила и процедуры резервирования программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций

6.1. Резервирование информационных ресурсов в ИСПДн ПетрГУ осуществляется в соответствии с Инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных и Регламентом резервного копирования соответствующих ИСПДн.

6.2. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

6.3. В случае сбоев, отказов и аварий систем электроснабжения и других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ИСПДн ПетрГУ до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИСПДн ПетрГУ а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

6.4. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- пользователи корректно отключают и обесточивают свои рабочие места;
- администраторы ИСПДн корректно отключают и обесточивают серверы и сетевое оборудование;
- администратор ИСПДн предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ИСПДн ПетрГУ в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор ИСПДн восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.