|  |
| --- |
| Приложение 1УТВЕРЖДЕНЫ приказом НИУ ВШЭот 24.12.2020 № 6.18.1-01/2412-04 |

**Правила обеспечения информационной безопасности**

**Национального исследовательского университета**

**«Высшая школа экономики»**

1. **Общие положения**

Правила обеспечения информационной безопасности НИУ ВШЭ (далее – Правила) обеспечивают основу соблюдения защищенности информации.

В соответствии с Программой развития НИУ ВШЭ до 2030 года перед Национальным исследовательским университетом «Высшая школа экономики» (далее – университет или НИУ ВШЭ) стоит стратегическая задача создания на базе университета передового научно-образовательного, аналитического, консалтингового и проектного центра мирового класса.

Успех перехода на новый качественный уровень в образовании, управлении, аналитике, прогнозировании напрямую зависит от способности противостоять современным киберугрозам, которые могут не только помешать, но и нанести существенный ущерб материальным, интеллектуальным, репутационным активам университета.

Как ведущая российская образовательная организация высшего образования НИУ ВШЭ имеет этические, юридические и профессиональные обязанности по обеспечению соответствия информации, которой обладает университет, принципам конфиденциальности, целостности и доступности. НИУ ВШЭ гарантирует, что информация, которой владеет или за которую несет ответственность, защищена от ненадлежащего раскрытия, является точной, и может быть своевременно использована теми, кто должен иметь к ней доступ.

Информация, обрабатывающаяся в информационных системах НИУ ВШЭ, является важной для реализации целей университета. Информационно-телекоммуникационная инфраструктура позволяет пользователям совместно использовать программы и данные, что повышает возможность реализации угроз информационной безопасности. Поэтому вся информация и все составляющие информационно-телекоммуникационной инфраструктуры нуждаются в защите.

Для достижения указанных целей в университете на регулярной основе проводятся мероприятия, обеспечивающие защищенность информации.

Правила предназначены для создания основы для понимания всеми работниками и обучающимися НИУ ВШЭ юридических и этических обязанностей в отношении защиты информации и для обеспечения возможности собирать, использовать, хранить и распространять информацию соответствующим образом.

1. **Область применения**

В сферу действия Правил попадают все аппаратные, программные и информационные ресурсы, входящие в информационно-телекоммуникационную инфраструктуру НИУ ВШЭ (информационные системы, вычислительная инфраструктура и сети связи, размещенные как в локальной вычислительной сети, так и в облачной инфраструктуре).

На основе положений Правил разрабатываются локальные нормативные акты НИУ ВШЭ в сфере информационной безопасности, которыми должны руководствоваться все работники и обучающиеся НИУ ВШЭ. При заключении договоров с третьими лицами, в том числе разработчиками программных систем университета, работники НИУ ВШЭ обеспечивают включение в договоры условий, направленных на выполнение положений Правил и локальных нормативных актов НИУ ВШЭ, разработанных в целях их реализации.

1. **Цели обеспечения информационной безопасности**

Целью выполнения Правил является обеспечение состояния защищенности информационных ресурсов, выражающейся в обеспечении целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

Защита информационных ресурсов необходима для:

* защиты несовершеннолетних обучающихся НИУ ВШЭ от информации, причиняющей вред их здоровью и развитию;
* защита от информации, распространение которой в Российской Федерации запрещено;
* поддержания деловой репутации и обеспечения конкурентоспособности по отношению к ведущим зарубежным образовательным и исследовательским центрам;
* обеспечения защиты университета и связанных с ним субъектов информационных отношений, интересы которых могут быть затронуты при нарушении функционирования информационных систем и информационных сервисов университета.
* соблюдения требований законодательства РФ в области защиты информации.

Частными целями университета при реализации положений Правил являются:

* защита информации и информационных активов от угроз, которые могут привести к нарушению характеристик безопасности;
* минимизация и локализация последствий при воздействии угроз;
* развитие корпоративной культуры в области обеспечения информационной безопасности;
* поддержание уровня безопасности, соответствующего законодательству Российской Федерации;
* следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности c учетом обеспечения уровня безопасности, соответствующего законодательству Российской Федерации);
* обеспечение безопасности в каждой функциональной области корпоративной сети;
* обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
* обеспечение анализа регистрационной информации;
* предоставление пользователям необходимой и достаточной информации для сознательного поддержания режима безопасности.

Каждое лицо, включая работников и обучающихся, должно быть вовлечено в процесс достижения целей НИУ ВШЭ, связанных с обеспечением информационной безопасности.

1. **Задачи обеспечения информационной безопасности**

Деятельность по защите информации должна обеспечить минимизацию рисков при решении задач, стоящих перед университетом.

Под рисками университета в настоящем контексте понимается:

* получение обучающимися доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;
* нанесение ущерба деловой репутации НИУ ВШЭ;
* нарушение конфиденциальности информационных активов;
* воздействие на непрерывность цифровых процессов реализации образовательной деятельности, научной деятельности, информационно-аналитического и экспертного обеспечения деятельности Правительства Российской Федерации, прикладных исследований, научных разработок и других видов деятельности, предусмотренных Уставом НИУ ВШЭ.

Деятельность по защите информации должна проводиться с учетом внешних и внутренних угроз, т.е. в условиях наличия реальных или потенциально возможных событий, действий, процессов или явлений, которые могут нанести ущерб университету.

1. **Правовые и нормативные обязательства**

Университет добивается того, чтобы все реализуемые им мероприятия по организационной и технической защите информации осуществлялись на законных основаниях, в том числе в соответствии с законодательством Российской Федерации в области информации, информатизации и защиты информации, нормативными правовыми актами Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Российской Федерации, Федеральной службы безопасности Российской Федерации и Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, а также в соответствии с лучшими практиками отечественных и международных стандартов.

1. **Основные положения Правил обеспечения информационной безопасности**
	1. **Виды защищаемой информации**

Расстановка приоритетов в обеспечении информационной безопасности проводится для информации, рассматриваемой как объект правовых отношений.

В зависимости от определенных законодательством Российской Федерации категорий доступа к информации, информация, обрабатываемая в университете, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен (информация ограниченного доступа).

К информации ограниченного доступа в университете относится конфиденциальная информация в соответствии с Положением о защите конфиденциальной информации Национального исследовательского университета «Высшая школа экономики».

Для работы с конфиденциальной информацией приоритетами в обеспечении информационной безопасности для университета являются:

* конфиденциальность;
* целостность;
* доступность.

Для работы с общедоступной информацией приоритетами для университета являются:

* целостность;
* доступность.

* 1. **Структура нормативного регулирования отношений в сфере информационной безопасности в НИУ ВШЭ**

Правила является основополагающим документом университета, предназначенным для выражения позиции НИУ ВШЭ в области информационной безопасности.

Университет применяет Правила для раскрытия заинтересованным сторонам своего подхода в области обеспечения информационной безопасности для расстановки приоритетов, планирования ресурсов, достижения согласия и договоренностей между участниками информационного процесса по поводу практических методов реализации и механизмов системы защиты информации.

Для детализации принятого настоящими Правилами подхода по достижению целей обеспечения информационной безопасности в университете разрабатываются и применяются соответствующие локальные нормативные акты в сфере информационной безопасности (положения, регламенты и другие), размещаемые в открытом доступе на корпоративном сайте (портале) НИУ ВШЭ.

Все указанные документы в совокупности составляют политику информационной безопасности НИУ ВШЭ.

* 1. **Распределение обязанностей** **по защите информации**

Вопросы защиты информации должны быть реализованы на всех стадиях и всеми лицами в ходе взаимодействия субъектов информационных отношений и информационных систем (компонентов корпоративной информационно-телекоммуникационной инфраструктуры) в соответствии с распределением обязанностей по защите информации.

Распределение обязанностей по защите информации производится в соответствии с функциональной ролью, которую выполняют работники, обучающиеся, представители третьей стороны при разработке, внедрении и эксплуатации информационных систем университета.

По функциональному признаку участники процесса обеспечения информационной безопасности подразделяются на:

* лица или структурные подразделения/ единицы, обеспечивающие эксплуатацию информационных систем для выполнения функционального назначения информационной системы;
* лица или структурные подразделения/ единицы, обеспечивающие функционирование информационных систем посредством информационных технологий;
* лица или структурные подразделения/ единицы, обеспечивающие разработку, внедрение и эксплуатацию системы управления (менеджмента) информационной безопасности (далее – СМИБ).

Определение функциональных ролей для выполнения тех или иных функций обеспечения информационной безопасности производится в виде набора необходимых действий в информационной системе (далее – ИС), а также прав, необходимых для их исполнения.

* + 1. Функциональные роли в системе защиты информации, относящиеся к лицам, обеспечивающим эксплуатацию информационных систем:
1. **заказчик автоматизации** – руководитель (или назначенное лицо) структурного подразделения НИУ ВШЭ, деятельность которого автоматизируется и который ответственен за выполнение функционального бизнес-процесса структурного подразделения в информационной системе, являющийся уполномоченным владельцем данных, обрабатываемых в процессе деятельности.

В случае выполнения бизнес-процессов различными структурными подразделениями, не находящимися в непосредственном подчинении данного лица, эта роль назначается координирующему заказчику, ответственному за координацию выполнения бизнес-процессов.

Данная роль подразумевает распоряжение обрабатываемой в ИС информацией и распределение обязанностей по обработке информации между работниками структурного(ых) подразделения(й).

В зоне ответственности заказчика (координирующего заказчика) ИС находятся, в том числе, следующие вопросы обработки защищаемой информации и обеспечения информационной безопасности:

* определение перечня подлежащих защите сведений (данных), обрабатываемых в ИС при автоматизации функционального(ых) процесса(ов) в подразделении(ях);
* определение ценности защищаемой информации и уровня ущерба в случае нарушения заданного уровня обеспечения характеристик безопасности (конфиденциальности, целостности, доступности);
* назначение (согласование допуска) работников подразделения(й) к автоматизированной обработке информации и полномочий указанных лиц;
* участие в процессе определения степени критичности информационных систем (проведения классификации ИС);
* повышение осведомленности администраторов и пользователей ИС по вопросам информационной безопасности.
1. **администратор ИС** – работник(и) структурного подразделения НИУ ВШЭ, ответственный за логику функционирования и настройку бизнес-процессов (функциональных процессов) в информационных системах.

В зоне ответственности администратора ИС находятся, в том числе, следующие вопросы обработки защищаемой информации и обеспечения информационной безопасности:

* настройка регистрации (логирования) действий пользователей ИС с информацией (ресурсами) штатными средствами прикладного программного обеспечения ИС;
* участие в процессах проверки эффективности системы защиты, реагирования на инциденты информационной безопасности.
1. **администратор данных ИС** – работник(и) структурных подразделений НИУ ВШЭ, ответственный(ые) за управление доступом в информационной системе. Данная роль может быть совмещена с ролью «администратор ИС».

В зоне ответственности администратора данных ИС находятся, в том числе, следующие вопросы обработки защищаемой информации и обеспечения информационной безопасности:

* настройка доступа к данным (информации) пользователей ИС (реализация правил разрешительной системы доступа штатными средствами ИС);
1. **ключевой пользователь ИС** – работник(и) структурных подразделений НИУ ВШЭ, работающий(ие) в информационной системе для выполнения функциональных обязанностей.

В зоне ответственности ключевого пользователя ИС находятся в том числе вопросы:

* непосредственной обработки информации в соответствии с правилами обеспечения информационной безопасности;
* участие в процессах проверки эффективности системы защиты, реагирования на инциденты информационной безопасности.
	+ 1. Роли в системе защиты информации, относящиеся к лицам, обеспечивающим функционирование информационных систем:
1. **владелец ИС** – работник структурного подразделения НИУ ВШЭ, обеспечивающий создание, модернизацию и внедрение информационной системы по заявкам заказчиков автоматизации.

В зоне ответственности владельца ИС находятся в том числе следующие вопросы обеспечения информационной безопасности:

* участие в процессе определения степени критичности информационных систем (проведения классификации ИС);
* организация обработки информации в ИС в соответствии с требованиями по защите информации;
* формирование правил разрешительной системы доступа ключевым пользователям ИС к обрабатываемой информации (данным) на основе полномочий, предоставленных заказчиком ИС;
* реализация организационных мер по защите информации в ИС на этапах разработки, внедрения и эксплуатации;
* организация реализации технических мер по защите информации в ИС на этапах разработки, внедрения и эксплуатации;
* участие в процессах проверки эффективности системы защиты, реагирования на инциденты информационной безопасности;
* повышение осведомленности администраторов и пользователей ИС по вопросам информационной безопасности.
1. **системный администратор ИС** – работник структурного подразделения НИУ ВШЭ (привилегированный пользователь ИС), обеспечивающий настройку и функционирование аппаратных и программных ресурсов информационной системы.

В зоне ответственности системного администратора ИС находятся в том числе следующие вопросы обеспечения информационной безопасности:

* администрирование штатных аппаратных ресурсов и специального программного обеспечения ИС в соответствии с требованиями по защите информации (требованиями технического задания на систему защиты или задания по безопасности);
* мониторинг (контроль) функционирования средств, находящихся в зоне ответственности, в соответствии с установленными правилами;
* участие в процессах проверки эффективности системы защиты, реагирования на инциденты информационной безопасности.
1. **администратор информационной безопасности ИС** – работник структурного подразделения НИУ ВШЭ (привилегированный пользователь ИС), обеспечивающий настройку и функционирование средств защиты информации.

В зоне ответственности администратора информационной безопасности ИС находятся в том числе следующие вопросы обеспечения информационной безопасности:

* администрирование наложенных (внешних по отношению к штатным средствам ИС) аппаратных и программных средств защиты информации, реализующих требования технического задания на систему защиты или задания по безопасности;
* мониторинг (контроль) функционирования средств, находящихся в зоне ответственности, в соответствии с установленными правилами;
* участие в процессах проверки эффективности системы защиты, реагирования на инциденты информационной безопасности.
	+ 1. С целью снижения рисков нарушения информационной безопасности и управления ими в НИУ ВШЭ создаются специальные структурные подразделения, которые организуют эксплуатацию и развитие системы управления (менеджмента) информационной безопасности университета. Работники данных подразделений разрабатывают и реализуют управленческие меры обеспечения информационной безопасности и выбирают эффективные средства защиты.

Роль в системе обеспечения информационной безопасности, относящаяся к подразделениям и лицам, обеспечивающим управление (менеджмент) системой обеспечения информационной безопасности:

1. **администратор СМИБ ИС** – работник центра информационной безопасности, обеспечивающий функционирование СМИБ информационной системы.

В зоне ответственности администратора СМИБ ИС находятся в том числе следующие вопросы обеспечения информационной безопасности:

* + организация планирования и проведение оценки рисков информационной безопасности;
	+ методологическая разработка и актуализация документов, составляющих политику информационной безопасности НИУ ВШЭ;
	+ планирование и контроль, организация обучения в области информационной безопасности;
	+ организация управления инцидентами информационной безопасности;
	+ проведение контрольных мероприятий, анализ защищенности и проверка эффективности системы защиты информации;
	+ аудит информационной безопасности, анализ функционирования системы обеспечения информационной безопасности, планирование изменений;
	+ распределение и контроль выполнения обязанностей по реализации мер обеспечения информационной безопасности;
	+ распределение соответствующих обязанностей между подразделениями и лицами, обеспечивающим создание и эксплуатацию системы защиты информации;
	+ выбор средств управления и обеспечения информационной безопасности.

Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы мероприятий в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Основой этой программы является многоуровневая политика информационной безопасности, отражающая комплексный подход университета к защите своих ресурсов и информационных активов.

1. **Ответственность**

Нарушение Правил обеспечения информационной безопасности может подвергнуть рискам информационную инфраструктуру университета и обрабатываемую в ней информацию. Случаи нарушения безопасности со стороны работников, преподавателей и обучающихся должны оперативно рассматриваться для решения вопроса о применении мер ответственности (дисциплинарного, гражданско-правового, административного или уголовного характера в соответствии с действующим законодательством РФ).