УЧРЕЖДЕНИЕ «ESIL UNIVERSITY»

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ESIL
UNIVERSITY

Утверждено Советом директоров
Учреждения «Esil University»
Протокол № 4 от «12» мая 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ “ESIL UNIVERSITY”

П EsU 13-02

Астана
2023

Политика информационной безопасности Учреждения «Esil University»

Согласовано на заседании Ученого Совета Учреждения «Esil University» (протокол № 10 от «30» марта 2023 г.)

Содержание

1. Общие положения

1.1 Политика информационной безопасности (далее – Политика) Учреждения Esil University (далее – Учреждение EsU) определяет систему взглядов на проблему обеспечения информационной безопасности (далее – ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее – СУИБ) Учреждения EsU.

1.2 Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Учреждения EsU. Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Учреждение EsU.

1.3 Настоящая политика разработана на основе требований законодательства Республики Казахстан, накопленного в Учреждении EsU опыта в области обеспечения ИБ, интересов и целей Учреждения EsU.

1.4 Настоящая Политика распространяется на все бизнес-процессы Учреждения EsU и обязательна для применения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов.

1.5 Настоящая Политика распространяется на информационные системы Учреждение EsU . Лица, осуществляющие разработку внутренних документов Учреждение EsU, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

1.6 Настоящая Политика является внутренним нормативным документом по ИБ.

1.7 Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий

2. Цель и задачи Политики информационной безопасности Учреждения «Esil University»

2.1.Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от

возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носителей, процессы обработки и передачи, а также минимизация рисков ИБ.

2.2.Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз ИБ;

– создание механизма оперативного реагирования на угрозы ИБ;

– предотвращение и/или снижение ущерба от реализации угроз ИБ;

– защита от вмешательства в процесс функционирования ИС посторонних лиц;

– соответствие требованиям законодательства, нормативно-методических документов и договорным обязательствам в части ИБ;

– обеспечение непрерывности критических бизнес-процессов;

– достижение адекватности мер по защите от угроз ИБ;

– выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;

– повышение деловой репутации и корпоративной культуры.

3. Термины и определения

3.1 Термины и определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Администратор безопасности - должностное лицо, назначаемое директором Центра информационных технологий, устанавливающее политику безопасности и идентифицирующее объекты и участников, к которым применяется эта политика.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждение EsU .

Владелец информационных ресурсов, информационных систем,

технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Документ – зафиксированная на материальном и электронных носителях информация с реквизитами, позволяющими её идентифицировать.

Доступность информации – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность (ИБ) – состояние защищённости интересов Учреждение EsU .

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный ресурс (актив) – всё, что имеет ценность и находится в распоряжении Учреждение EsU .

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан.

Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

ПО – программное обеспечение

Политика – общие цели и указания, формально выраженные руководством.

Привилегии – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

Риск – сочетание вероятности события и его последствий.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.

События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Угроза – Опасность, предполагающая возможность потерь (ущерба).

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

ЦИТ – Центр информационных технологий

4 Основная часть

4.1 Информационные ресурсы и управление привилегиями

В Учреждении EsU должны быть выявлены и оценены с точки зрения их важности все информационные ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Учреждение EsU реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В ИС Учреждения EsU присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Учреждение EsU ;
- открыто распространяемая информация, необходимая для работы Учреждение EsU , независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки,

передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Руководство Учреждение EsU должно требовать от всех пользователей принятия мер безопасности в соответствии с установленными в Учреждении EsU политиками и процедурами. Уполномоченные руководством Учреждение EsU сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования сотрудниками информационных ресурсов;
- Содержания служебной переписки.

К пользователям информационных ресурсов относятся:

- разработчики прикладного программного обеспечения, технические специалисты, системные администраторы (специалисты по информационной безопасности) и др.;
- сотрудники, осуществляющие свою деятельность в Университете и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
- студенты, магистранты и докторанты.
- потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Университета.

Уровень полномочий каждого пользователя определяется в соответствии с уровнем доступа и определяется в должностных инструкциях . Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями. Каждому пользователю, допущенному к работе с конкретным информационным активом Учреждения EsU, предоставляется персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИА.

Управление привилегиями

Доступ сотрудника к информационным ресурсам Учреждения EsU должен быть санкционирован соответствующим, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения EsU осуществляется в процессе аудита ИБ сотрудниками ЦИТ.

Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

•все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;

•необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;

•пароли должны храниться в электронном виде;

Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

•права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;

•необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Учреждения EsU предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации. Не допускается использование различными пользователями одних и тех же учётных данных. Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности.

Личные пароли устанавливаются первый раз сотрудниками отдела ЦИТ. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

•длина пароля должна быть не менее 8 символов;

•в числе символов пароля должны присутствовать три из четырёх видов символов:

•буквы в верхнем регистре;

•буквы в нижнем регистре;

•цифры;

•специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);

Сотруднику запрещается:

•сообщать свой пароль кому-либо;

•указывать пароль в сообщениях электронной почты;

•хранить пароли, записанные на бумаге, в легко доступном месте;

•использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

•использовать один и тот же пароль для доступа к различным корпоративным ИС;

•удалять служебную информацию со своего компьютера любыми способами.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Сотрудник обязан:

•в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику отдела ИС СМТ;

•немедленно сообщить сотруднику отдела ЦИТ в случае получения от кого-либо просьбы сообщить пароль;

•менять пароль каждые 90 дней;

•менять пароль по требованию Администратора безопасности

Учреждение EsU оставляет за собой право:

•осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;

•принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей Политики.

Сотрудники Учреждения EsU обязаны:

•сохранять известные им пароли в тайне;

•закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;

•по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

4.2 Использование ресурсов сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения EsU, базы данных, электронная почта. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы.

Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

•знать и выполнять требования по работе с конфиденциальной информацией;

•при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения EsU применять средства защиты от неавторизованного доступа;

•не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;

•обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;

•не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;

•не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;

•не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

Корпоративная электронная почта Учреждения EsU предназначена исключительно для использования в служебных целях. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Учреждению EsU. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Учреждению EsU и являются неотъемлемой частью его производственного процесса. Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Учреждения EsU либо удалены уполномоченными сотрудниками Учреждения EsU.

Пользователям корпоративной электронной почты Учреждения EsU запрещено вести частную переписку с использованием средств корпоративной электронной почты Учреждения EsU.

Работа в сети

Общедоступные ресурсы (почтовые сервера, web-сервера, web- порталы и другие ресурсы) должны быть размещены в отдельном сегменте ЛВС университета. Подключение указанных ресурсов к Интернет осуществляется через Единый шлюз доступа в сеть Интернет (ЕШДИ). При этом должны применяться межсетевые экраны и системы обнаружения и предотвращения вторжений (IDP, IPS, Anti-DDoS).

Доступ к сети Интернет предоставляется сотрудникам Учреждения EsU в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам. Для

доступа сотрудников Учреждения EsU к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

•соблюдать требования настоящей Политики;

•использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;

•ставить в известность отдел ЦИТ о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

•использовать предоставленный Учреждением EsU доступ в сеть Интернет в личных целях;

•использовать несанкционированные аппаратныеи программные средства, позволяющие получить несанкционированный доступ к сети Интернет;

•Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения EsU;

•Публиковать, загружать и распространять материалы содержащие: конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ; угрожающую, клеветническую, непристойную информацию;

•вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;

•фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Учреждение EsU оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Информация о посещаемых сотрудниками Учреждения EsU Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена руководителям структурных подразделений, а также руководству Учреждения EsU для контроля. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

4.3 Аудит информационной безопасности

Соблюдение требований Положения информационной безопасности обязательно для всех пользователей информационных систем Университета.

Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых пунктов Положения и внесения в них необходимых корректировок.

Аудит информационной безопасности Университета целесообразно проводить ежегодно, по итогам которого директором ЦИТ и главным системным администратором по информационной безопасности должен проводиться пересмотр Положения на предмет соответствия предъявляемым требованиям, в случае возникновения необходимости вносить изменения и дополнения.

Учреждение должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

С целью контроля обеспечения конфиденциальности

- ежегодная сверка списка официально зарегистрированных пользователей и пользователей, работающих в ИС.
- ежегодный аудит ИБ на соблюдение требований настоящего Положения.
- постоянный мониторинг инструментальными, программными средствами ИБ Информационно-коммуникационной инфраструктуры университета.
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники Учреждения EsU при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

Ответственность

Директор ЦИТ Учреждения EsU определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Учреждения EsU. Ответственность за поддержание положений настоящей Политики в

актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Учреждения EsU лежит на руководстве отдела ЦИТ. Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях. Работники Учреждения EsU несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ЦИТ.

Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, маршрутизатор, файервол) должны находиться в отдельном помещении. Помещение должно быть оборудовано принудительной вентиляцией, пожарной сигнализацией и системой автоматического пожаротушения. Доступ в помещение посторонним лицам запрещен, строго фиксируется, отмечается в журнале и имеют право проводить работы только с разрешения курируемого проректора или директора ЦИТ. Круг сотрудников, имеющих доступ к серверам Учреждения EsU строго регламентируется должностными инструкциями. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении для выполнения своих должностных обязанностей.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей. Руководство Учреждения EsU регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ. Нарушение требований нормативных актов Учреждения EsU по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

Требования к управлению инцидентами безопасности

О случаях нарушения ИБ следует сообщать незамедлительно ответственному лицу за ИБ. Должны быть установлены зоны ответственности и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе защиты информации. Должны быть приняты механизмы для ведения мониторинга инцидентов в системе защиты информации и постоянно их контролировать.

Требования к отказоустойчивости

- Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС университета со временем однократного простоя не более 10 часов и суммарным временем простоя не более 48 часов в год.

•В случае возникновения внештатной ситуации, произошедшей с производственным сервером ИС, восстановление ПО, системного ПО и ОС должно быть произведено в течение 12 часов.

•Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов, проверку состояния резервных батарей, без вмешательства администратора и без влияния на работу пользователей.

•В целях защиты информации от преднамеренного или непреднамеренного ее уничтожения и фальсификации должно быть обеспечено обязательное резервирование всей информации, являющейся важной.

•Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

•Бесперебойное электропитание обеспечивается источником бесперебойного питания (ИБП) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и ОС при отключении внешнего электропитания.

5.Заключительные положения

5. 1. Настоящее Политика и вносимые в неё изменения и дополнения вводятся в действие с момента их утверждения Советом директоров по согласованию с Ученым совете Учреждения EsU .

5. 2. Ответственный за аудит документа – Ученый секретарь.

5. 3. Ответственность за хранение несет Отдел обеспечения качества и стратегического анализа.

Лист согласования

Должность	Ф.И.О.	Дата	Подпись
Проректор по СиЦ	Шуйтенов Г.Ж.	29.03.2023	
Директор ЦИТ	Акпаров Ж.А.	29.03.2023	
Юрист	Имамбаева Р.Г.	29.03.2023	
Начальник ООКиСА	Данириова М.Т.	29.03.2023	