УТВЕРЖДЕНО
приказом ООО «Европ Ассистанс СНГ»
от 03.06.2019 № 1-2019-СУИБ

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Политика управления информационной безопасностью

Версия 1.0

Разработано:	Червонный Станислав Олегович	13.05.2019
Утверждено:	Пиомбо Вадим	03.06.2019

Содержание

1 Назначение и область применения

Настоящая Политика системы управления информационной безопасностью (далее – Политика) устанавливает общие требования к процессам и системе управления информационной безопасностью (далее – СУИБ) ООО «Европ Ассистанс СНГ» (далее – Компания) в целом, а также определяет основные принципы и подходы к обеспечению информационной безопасности (далее – ИБ).

Требования настоящей Политики являются обязательными для исполнения работниками всех структурных подразделений Компании, подрядчиков и контрагентов, допущенных к активам Компании

2 Термины и сокращения

В настоящей Политике используются следующие термины с соответствующими определениями:

«актив» – все, что имеет ценность для Компании; к активам относятся: информация, информационные системы (включая их отдельные компоненты, такие как программное обеспечение, оборудование, услуги, предоставляемые третьими лицами), работники Компании и т. д.;

«владелец актива» – работник Компании, уполномоченный управлять созданием, разработкой, поддержанием, использованием и защитой активов;

«владелец процесса» – работник Компании, имеющий в своем распоряжении ресурсы, необходимые для выполнения процесса, и несущий ответственность за соблюдение правил выполнения и результат процесса;

«доступность» – свойство актива, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно;

«информационная безопасность» – сохранение конфиденциальности, целостности и доступности информации;

«информационная система» – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

«информация» – сведения (сообщения, данные) независимо от формы их представления;

«ИТ-инфраструктура» – все аппаратное и программное обеспечение, сети, инженерное обеспечение и т. п., необходимые для разработки, тестирования, предоставления, мониторинга, контроля или поддержки ИТ-услуг. Термин ИТ-инфраструктура включает в себя все компоненты информационных технологий, но не включает связанные с ними процессы и документацию, работников Компании и третьих лиц;

«конфиденциальность» – свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;

«менеджер по ИБ» - ответственный за формирование и реализацию решений определенных задач, направленных на противодействие угрозам информационной безопасности Компании. Назначается приказом Компании.

В тексте документа использованы следующие сокращения:

ИБ	- Информационная безопасность
ИТ	- Информационные технологии
СУИБ	- Система управления информационной безопасности
ОД	- Область деятельности

3 Общие положения

Одним из важнейших активов Компании является информация, значимая для ее деятельности, в том числе используемая в ходе взаимодействия с клиентами и партнерами.

Нарушение применимых требований ИБ может привести к серьезным последствиям, таким как финансовые потери, правовые санкции, ущерб репутации Компании, в том числе потеря доверия со стороны клиентов и партнеров, снижение конкурентоспособности.

Надлежащий уровень ИБ в Компании обеспечивается в соответствии с требованиями бизнеса, требованиями законодательства и регуляторов в части ИБ путем внедрения и непрерывного совершенствования СУИБ на основе международных стандартов и практик.

4 Область деятельности СУИБ

Для эффективной реализации процессов обеспечения ИБ в Компании внедряется СУИБ, соответствующая требованиям международного стандарта ISO/IEC 27001:2013.

СУИБ распространяется на ключевые бизнес-процессы, безопасность и непрерывность которых важно обеспечить для стабильного функционирования всей Компании.

СУИБ Компании применяется к – «предоставлению и администрированию механической и электротехнической гарантии на транспортные средства новые и с пробегом.

Организации помощи на дорогах владельцам транспортных средств, организации медицинской помощи в России и за рубежом». Описание данных бизнес-процессов, входящих в них подразделений и активов, а также обоснование выбора данных бизнес-процессов в качестве области деятельности СУИБ приведены в документе «Область деятельности СУИБ».

5 Цели и задачи СУИБ

Основная цель СУИБ – создание и постоянное поддержание в Компании условий, при которых риски, связанные с обеспечением безопасности активов Компании, постоянно контролируются и находятся на приемлемом уровне.

Достижение данной цели позволяет:

- защитить активы Компании от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных);
- обеспечить непрерывность бизнеса;
- обеспечить соответствие Компании требованиям действующего законодательства и регуляторов в области ИБ;
- обеспечить соответствие процессов обеспечения ИБ бизнес-требованиям Компании;
- минимизировать ущерб, наносимый бизнесу в результате возникновения инцидентов ИБ;
- обеспечить доверие клиентов и партнеров Компании.

Вышеописанная цель достигается решением следующих задач:

- инвентаризация активов Компании и регулярное проведение оценки рисков ИБ;
- применение обоснованных, экономически эффективных организационных и технических мер по обеспечению ИБ;

- выявление применимых требований действующего законодательства и регуляторов в области ИБ, достижение соответствия этим требованиям;
- установление ответственности работников по вопросам обеспечения ИБ, обучение и повышение их осведомленности в части ИБ;
- регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов СУИБ, мониторинга эффективности процессов СУИБ, анализа СУИБ руководством Компании;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям;
- подтверждение соответствия СУИБ Компании требованиям международного стандарта ISO/IEC 27001:2013.

6 Принципы СУИБ

В процессе обеспечения ИБ Компания руководствуется принципами, приведенными ниже.

- Законность. При обеспечении ИБ выполняются требования применимого законодательства, а также действующие нормативные требования государственных регулирующих органов, в том числе, международных.
- Адекватность существующим угрозам и экономическая обоснованность. Применяемые организационные и технические меры защиты выбираются исходя из потребностей бизнеса на основе результатов анализа и оценки рисков ИБ, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение мер управления рисками. Проводится периодическая оценка эффективности используемых мер и механизмов защиты.
- Минимизация ограничивающего влияния на бизнес-процессы. Применяемые организационные и технические меры СУИБ минимально влияют на функционирование и характеристики бизнес-процессов Компании.
- Перспективность и ориентация на существующие российские и международные открытые стандарты. Организационные и технические меры СУИБ реализуются с учетом мировых тенденций в области ИБ. Ориентация на открытые стандарты позволяет использовать накопленный мировой опыт в области защиты информации, а также обеспечивает прозрачность процессов ИБ и простоту взаимодействия в рамках задач по обеспечению ИБ.
- Непрерывность функционирования. Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СУИБ.
- Непрерывность совершенствования. Для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СУИБ.
- Персональная ответственность. Каждый работник Компании несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СУИБ.
- Контроль. Осуществляется постоянный контроль выполнения работниками Компании требований в области ИБ.

7 Стратегическое управление СУИБ

Деятельность по обеспечению ИБ в Компании планируется ежегодно на уровне высшего руководства. Ресурсы на поддержку и модернизацию СУИБ регулярно выделяютя высшим руководством.

Ответственность за ИБ четко определена и документирована.

8 Определение ролей и ответственности

Для достижения заявленных целей Компании в сфере ИБ для работников и представителей сторонних организаций определены роли.

Требования к порядку назначения работников на роли, зонам их ответственности детально документированы в нормативных документах Компании.

9 Управление рисками

В соответствии с риск-ориентированным подходом, устанавливаемым настоящей Политикой, в Компании регулярно проводиться инвентаризация активов, категорирование информации, а также анализ и оценка рисков в соответствии с разработанной процедурой управления рисками ИБ, которая предусматривает идентификацию, анализ и оценку рисков ИБ, обработку неприемлемых рисков.

Результаты оценки рисков, состав применяемых в Компании мер обеспечения ИБ и планы по обработке рисков сформированы в соответствии с принятыми в Компании методиками по управлению рисками ИБ.

Ответственность за пересмотр рисков, за разработку и контроль исполнения мероприятий по минимизации рисков, за утверждение критериев принятия рисков ИБ определена и документирована.

10 Управление документацией СУИБ

Разработка, оформление, согласование, регистрация, хранение, передача и уничтожение документации, относящейся к СУИБ Компании, соответствует принятым в Компании требованиям по управлению организационно-распорядительной документацией.

Доступ к документации, представленной как на печатных носителях, так и в электронном виде и содержащей конфиденциальную информацию, ограничен и предоставляться только тем работникам Компании, контрагентам и партнерам, которые прошли необходимые процедуры получения соответствующих прав доступа.

В поддержку организационно-распорядительной документации СУИБ Компании создаются записи, которые являются свидетельствами выполнения процессов управления и обеспечения ИБ и результативности функционирования СУИБ Компании в целом.

11 Обучение персонала

Работники Компании регулярно проходят обучение (повышение уровня знаний) в области ИБ.

Работники Компании, ответственные за определение и контроль требований по ИБ, постоянно поддерживают уровень своей компетенции, принимая участие в различных выставках, форумах и конференциях по ИБ, изучая методики, признанные лучшими мировыми практиками, а также используя источники массовой информации.

Проводится регулярный контроль знаний работников Компании в области ИБ.

12 Организация работы со сторонними организациями

Компания в процессе своей деятельности взаимодействует со следующими сторонними организациями:

- клиенты и контрагенты;
- международные и российские регуляторы;
- государственные органы;
- организации группы Europ Assistance.

При заключении договоров со сторонними организациями необходимо учитывать требования ИБ обеих сторон. Согласованные требования по ИБ, касающиеся порядка обмена, обработки, хранения и распространения информации, предоставления доступа сторонних организаций к активам Компании зафиксированы в договоре и/или соглашении о конфиденциальности.

В договоре с контрагентами, оказывающими услуги по обеспечению физической безопасности и обслуживанию ИТ-инфраструктуры Компании, учтены требования к порядку осуществления доступа на территорию, в помещения и к активам Компании.

Взаимодействие с международными и российскими регуляторами, государственными органами регламентируются соответствующими федеральными законами и другими нормативно-правовыми актами Российской Федерации, применимым международным законодательством.

13 Внутренние аудиты ИБ

В Компании регулярно (не реже раза в год) проводятся внутренние аудиты СУИБ с целью проверки того, что процессы, процедуры и меры обеспечения ИБ:

- соответствуют требованиям нормативных документов СУИБ;
- соответствуют требованиям ISO/IEC 27001:2013, а также требованиям действующего законодательства;
- реализованы и сопровождаются в соответствии с установленными целями и задачами ИБ.

Критерии, область аудита, частота, методы проведения, ответственность, требования к планированию и проведению аудитов в Компании, а также к предоставлению отчетов по результатам и ведению записей определены и документированы.

Выбор аудиторов и проведение аудитов гарантируют объективность и непредвзятость процесса аудита. Аудиторы не проверяют свою собственную работу.

Выявленные в ходе внутренних аудитов несоответствия и их причины устраняются корректирующими мероприятиями.

Доступ к техническим средствам проведения аудита защищен с целью предотвращения возможного ненадлежащего использования и компрометации. Доступ к результатам аудита со стороны работников Компании и/или работников сторонних организаций ограничен.

14 Мониторинг, анализ эффективности и совершенствование процессов СУИБ

В Компании проводиться регулярный мониторинг процессов СУИБ с целью:

- быстрого обнаружения ошибок, отклонений и несоответствий в результатах обработки информации, выполнении процессов обеспечения и управления ИБ, а также выявления причин этих отклонений;
- быстрого выявления удавшихся и неудавшихся попыток нарушений и инцидентов ИБ;

- оценки эффективности мероприятий, предпринятых для совершенствования СУИБ (путем введения специальных показателей эффективности).

В Компании регулярно, не менее двух раз в год, проводится анализ СУИБ. При этом учитываются результаты проведения аудитов безопасности, статистика и дополнительная информация по произошедшим инцидентам ИБ, результаты оценки эффективности процессов ИБ, а также предложения и комментарии от всех заинтересованных сторон.

В Компании непрерывно совершенствуется СУИБ путем применения корректирующих мер, определенных по результатам анализа СУИБ. Порядок выбора, согласования и применения корректирующих мер документирован.

15 Соответствие требованиям законодательства

В Компании обеспечивается соблюдение требований законодательства и договорных отношений в области использования материалов, охраняемых правом интеллектуальной собственности, а также в области использования коммерческого программного обеспечения.

В Компании допустимо к использованию только лицензионное программное обеспечение.

В Компании определены и реализованы требования к обработке и обеспечению безопасности персональных данных в соответствии с действующим законодательством, требованиями и рекомендациями регулирующих органов.

Требования к сбору, систематизации, уточнению, хранению, использованию, распространению, обезличиванию, блокированию и уничтожению персональных данных определены в нормативных документах Компании.

16 Порядок внесения изменений

Ответственным за актуализацию Политики является Менеджер по ИБ.

Настоящая Политика пересматривается не реже, чем раз в три года.

Внеплановый пересмотр настоящей Политики может осуществляться также в следующих случаях:

- при существенном изменении организационной структуры Компании, структуры активов и применения новых технологий передачи, хранения и обработки информации;
- по результатам проведения проверки соответствия ИБ (аудит, оценка эффективности);
- по результатам анализа произошедших инцидентов ИБ;
- по результатам анализа рисков ИБ.

17 Контроль за исполнением Политики

Общее руководство и контроль исполнения положений настоящей Политики возложены на генерального директора Компании.

Лист регистрации изменений

Изменение №	Измененные листы			Версия документа до внесения изменений	Версия документа после внесения изменений	Утверждающий документ	Ф.И.О. и подпись внесшего изменение
	Общее кол-во	№ листа	Краткое описание				