УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____
А.А. Сташевский
20.06.2023

ПОЛИТИКА
информационной безопасности
(кибербезопасности)
ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (кибербезопасности) ООО «Файнекс» (далее – Политика) разработана в соответствии с Положением о требованиях, которым должны соответствовать отдельные заявители для регистрации их в качестве резидентов Парка высоких технологий (далее – ПВТ), утвержденным решением Наблюдательного совета ПВТ, а также в соответствии с требованиями законодательства о защите информации и с учетом практик, сложившихся в сфере защиты информации, таких, как стандарты из семейства ISO/IEC 27.

1.2. Настоящая Политика определяет основные цели, задачи, объекты защиты, процессы обеспечения информационной безопасности (кибербезопасности) в ООО «Файнекс» (далее – Организация), а также функции и обязанности органов управления и должностных лиц, участвующих в процессах обеспечения информационной безопасности Организации.

1.3. Для целей настоящей Политики нижеприведенные термины используются в следующих значениях:

информационная безопасность (кибербезопасность), ИБ – состояние защищенности информационных активов от случайных и преднамеренных угроз, в результате реализации которых в том числе возможно нарушение свойств доступности, целостности и (или) конфиденциальности информационных активов, хищение и совершение иных противоправных действий в отношении цифровых знаков (токенов) в информационной системе Организации, перебои в работе информационной системы;

информационные активы – информация, информационная система Организации, цифровые знаки (токены) в информационной системе Организации, используемые Организацией при осуществлении своей деятельности;

информация – обрабатываемая, хранящаяся и (или) передаваемая Организации информация (в том числе информация, распространение и (или) предоставление которой ограничено, относящаяся к клиентам Организации);

информационная система Организации – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-

технических средств, используемая Организацией для осуществления своей деятельности;

конфиденциальность информационных активов – свойство ИБ, заключающееся в том, что обработка, хранение и (или) передача информационных активов осуществляется таким образом, что информационные активы доступны только авторизованным (санкционированным) пользователям, объектам системы или процессам;

клиенты – контрагенты, с которыми Организация совершает сделки (операции), предусмотренные в его бизнес-проекте, либо которые обратились к нему за совершением таких сделок (операций);

целостность информационных активов – свойство ИБ сохранять неизменность или обнаруживать факт изменения (в том числе несанкционированного) в своих информационных активах;

доступность информационных активов – свойство ИБ, заключающееся в том, что информационные активы (доступ к ним) предоставляются авторизованному (санкционированному) пользователю в виде и месте, необходимом пользователю, а также в то время, когда они ему необходимы;

система ИБ – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное обеспечение, нацеленных на обеспечение ИБ в Организации;

системный администратор – работник Организации, в должностные обязанности которого входит, в том числе, администрирование и обеспечение работоспособности информационной системы Организации;

средства защиты – технические, программные, программно-аппаратные средства, предназначенные для защиты информации, цифровых знаков (токенов) и обеспечения бесперебойной работы информационной системы Организации, а также средства контроля эффективности такой защиты;

риск нарушения ИБ – риск, связанный с угрозой ИБ;

защитная мера – сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ Организации;

угроза ИБ – угроза нарушения свойств ИБ (доступности, целостности или конфиденциальности) информационных активов Организации, а также угроза совершения хищения и иных противоправных действий в отношении цифровых знаков (токенов) в информационной системе Организации, перебоев в работе информационной системы Организации;

уязвимость ИБ – слабость в инфраструктуре Организации, в том числе в системе обеспечения ИБ, которая может быть использована для реализации или способствовать реализации угрозы ИБ;

ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Организации или другой вред активам и (или) инфраструктуре Организации, наступившие в результате реализации угроз ИБ через уязвимости ИБ;

инцидент ИБ – событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ;

план работ по обеспечению ИБ – документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению ИБ, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей;

аудит ИБ – периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в Организации установленных требований по обеспечению ИБ.

1.4. Иные термины, используемые в настоящей Политике, и не указанные в пункте 1.3, имеют значения, определенные нормативными правовыми (техническими нормативными правовыми) актами Республики Беларусь, актами Наблюдательного совета ПВТ, локальными правовыми актами Организации (далее – ЛПА).

1.5. В случаях, если отдельные нормы Политики противоречат законодательству Республики Беларусь, актам Наблюдательного совета ПВТ, данные нормы утрачивают силу и применяются соответствующие нормы законодательства Республики Беларусь, актов Наблюдательного совета ПВТ до внесения необходимых изменений в Политику. Недействительность отдельных норм Политики не влечет недействительность других норм Политики и Политики в целом.

1.6. Во всем ином, что не предусмотрено Политикой, Организация руководствуется законодательством Республики Беларусь, актами Наблюдательного совета ПВТ и иными ЛПА Организации.

1.7. Взаимодействие информационной системы Организации с внешними информационными системами осуществляется в соответствии с регламентами информационного взаимодействия, утвержденными Организацией и собственниками внешних информационных систем. При осуществлении взаимодействия с внешними информационными системами должны соблюдаться требования по защите информации, установленные собственником информационной системы, осуществляющей передачу информации, распространение и (или) предоставление которой ограничено, во взаимодействующую информационную систему.

ГЛАВА 2
ЦЕЛИ, ЗАДАЧИ, ОБЪЕКТЫ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ ОРГАНИЗАЦИИ

2.1. Целями обеспечения ИБ являются предотвращение реализации угроз ИБ, предотвращение и (или) снижение ущерба от инцидентов ИБ, обеспечение условий для выполнения Организацией своих миссии, целей и задач.

2.2. Объектами ИБ являются информационные активы, реализация угроз в отношении которых может нанести ущерб Организации и (или) ее клиентам.

2.3. Основными задачами деятельности по обеспечению ИБ являются:

разработка требований по обеспечению ИБ;

контроль выполнения установленных требований по обеспечению ИБ;

повышение эффективности мероприятий по обеспечению и поддержанию ИБ;

разработка и совершенствование правовой базы Организации по обеспечению ИБ;

выявление, оценка и прогнозирование угроз и рисков ИБ;

организация процессов обеспечения ИБ.

2.4. Построение системы ИБ осуществляется на основе следующих принципов:

принцип осознанного принятия рисков. Риски объективно невозможно полностью ликвидировать, они могут снижаться или приниматься;

принцип разрешения (запрещено все, что не разрешено). Доступ к какому-либо объекту ИБ должен предоставляться только при наличии соответствующего правила, отраженного в соответствующем ЛПА, а также защитных и (или) контрольных мер;

принцип разграничения доступа. Каждому пользователю предоставляется доступ к информации и ее носителям в соответствии с его полномочиями;

принцип достаточной стойкости. Потенциальные злоумышленники при совершении попыток нанесения ущерба Организации должны встречать препятствия в виде достаточно сложных вычислительных задач, неадекватно больших временных затрат и (или) вычислительных мощностей.

ГЛАВА 3
ОБЩАЯ ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ИБ

3.1. На информационные активы, владельцем которых является Организация и которые вовлечены в технологические процессы, воздействуют внешние и внутренние угрозы, что обуславливает возникновение рисков нарушения ИБ.

3.2. Риски нарушения ИБ заключаются в возможности утраты целостности, конфиденциальности и (или) доступности информационных активов, вследствие чего Организации и ее клиентам может быть нанесен ущерб.

3.3. Риски нарушения ИБ являются видом операционного риска Организации, а система управления рисками нарушения ИБ является частью системы управления рисками Организации.

Цели, задачи, общая организация управления рисками нарушения ИБ Организации регламентированы Методикой управления риском нарушения информационной безопасности в ООО «Файнекс».

3.4. Угрозы ИБ могут быть природного, техногенного и антропогенного характера. Угрозы антропогенного характера могут быть как злоумышленные, так и незлоумышленные.

3.5. Угрозы ИБ объективно обусловлены наличием уязвимостей в информационной инфраструктуре Организации, основными из которых являются:

наличие вероятности допуска к работе в Организации пользователей, которые не являются лояльными по отношению к Организации;

наличие вероятности нарушения работниками Организации Правил информационной безопасности при работе пользователей в информационной системе Организации;

наличие вероятности технологических сбоев в работе компонентов информационной системы Организации;

наличие незадекларированных возможностей используемого программного обеспечения;

уязвимости системного и прикладного программного обеспечения, возникновение которых возможно в процессе эксплуатации и модернизации компонентов информационной системы Организации;

наличие вероятности возникновения ошибки в настройках компонентов информационной системы Организации;

наличие вероятности несвоевременной установки обновлений программного обеспечения, влияющей на ИБ.

3.6. Угрозы ИБ реализуются через организационно-технологическую инфраструктуру Организации, которая имеет следующие основные уровни:

физический (линии связи, аппаратные средства и др.);

сетевое оборудование (маршрутизаторы, коммутаторы, концентраторы и др.);

сетевые приложения и сервисы;

системное и прикладное программное обеспечение;

системы управления базами данных;

технологические процессы;

бизнес-процессы Организации.

3.7. С учетом имеющихся угроз и рисков нарушения ИБ в Организации реализуются организационные и технологические меры по защите информации.

ГЛАВА 4
ОРГАНИЗАЦИОННЫЕ И ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

4.1. Для защиты информации (в том числе информации, распространение и (или) предоставление которой ограничено, относящейся к клиентам) и цифровых знаков (токенов) в информационной системе Организации, реализуются следующие организационные и технологические меры.

4.2. Основными организационными мерами по защите информации являются:

определение должностного лица, ответственного за системное администрирование и информационную безопасность в Организации. Функциональные обязанности указанного должностного лица устанавливаются его должностной инструкцией;

выработка и реализация правил обращения с информацией ограниченного распространения, в том числе с персональными данными клиентов. Указанные правила установлены Положением об информации ограниченного распространения в ООО «Файнекс»;

реализация процессов обеспечения ИБ.

4.3. Основными процессами обеспечения ИБ являются:

организация учета информационных активов;

управление доступом работников к информационным активам, регистрация и контроль их действий;

управление портами ввода-вывода;

обеспечение сетевой безопасности;

обеспечение безопасной конфигурации и настроек компонентов информационной системы Организации;

обеспечение защиты от вредоносных программ и кодов;

обеспечение безопасного использования сети Интернет;

обеспечение криптографической защиты информации;

обеспечение ИБ технологических процессов;

управление уязвимостями компонентов информационной системы Организации;

управление инцидентами ИБ;

управление рисками нарушения ИБ;

обучение и повышение осведомленности работников Организации в области ИБ.

Порядок организации указанных процессов регламентируется отдельными ЛПА.

4.4. Основными технологическими мерами по защите информации являются:

применение средств технической и (или) криптографической защиты информации. Перечень средств указан в пункте 4.5 настоящей Политики;

ограничение круга лиц, имеющих право входа (доступа) в информационную систему заявителя. Данная мера регламентируется Положением по созданию автоматизированных рабочих мест и предоставлению доступа к информационным ресурсам ООО «Файнекс»;

применение многофакторной аутентификации при осуществлении входа (доступа) в информационную систему заявителя.

4.5. Для обеспечения ИБ Организации с учетом выявленных и потенциальных угроз и рисков нарушения ИБ будут использоваться средства технической и (или) криптографической защиты информации:

мониторинга событий системного и прикладного программного обеспечения;

предотвращения утечек информации ограниченного распространения из информационной системы Организации;

обнаружения и предотвращения вторжений;

защиты от вредоносных программ и кодов;

фильтрации и контроля интернет-трафика;

криптографической защиты информации и электронно-цифровой подписи;

сканирования уязвимостей;

централизованного управления доступом.

4.6. При наличии целесообразности и технических возможностей допускается использование Организацией средств технической и (или)

криптографической защиты информации, сервисов обеспечения ИБ сторонних организаций на договорной основе.

ГЛАВА 5
ОРГАНИЗАЦИОННЫЕ И ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕСПЕРЕБОЙНОЙ РАБОТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

5.1. Технологические и организационные меры, направленные на обеспечение бесперебойной работы информационной системы Организации, разрабатываются в соответствии с требованиями:

Положения о требованиях, которым должны соответствовать отдельные заявители для регистрации их в качестве резидентов Парка высоких технологий, утвержденного Решением Наблюдательного совета Парка высоких технологий;

Положения по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс».

5.2. Мероприятия по оперативному восстановлению работоспособности информационной системы после ее нарушения, в том числе после возникновения аварийных ситуаций (включая меры по восстановлению данных на случай их изменения или уничтожения), регламентированы Планом мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс».

ГЛАВА 6
МОНИТОРИНГ И ТЕСТИРОВАНИЕ СИСТЕМЫ ИБ

6.1. Для оценки защищенности информационной системы Организации и эффективности применяемых защитных средств проводится мониторинг и тестирование системы ИБ Организации.

6.2. Мониторинг системы ИБ Организации заключается в наблюдении, анализе, установлении причинно-следственных связей, которые предпринимаются Организацией в целях постоянной оценки фактического состояния системы ИБ для выявления на ранних стадиях и своевременного устранения либо предотвращения причин и условий, которые способствуют (могут способствовать) нарушению работы информационной системы Организации (повреждению, хищению данных).

Мониторинг системы ИБ проводится на постоянной основе и осуществляется в соответствии с Положением о мониторинге событий информационной безопасности в ООО «Файнекс».

6.3. Тестирование системы ИБ осуществляется посредством проведения внешних и внутренних тестов на проникновение.

В процессе проведения внешнего (внутреннего) теста на проникновение лица, осуществляющие тестирование, извне (изнутри) информационной системы Организации предпринимают попытки преодолеть элементы (средства) ее информационной безопасности, моделируя противоправное вмешательство (несанкционированный доступ) в работу информационной системы

Организации со стороны третьих лиц, направленное на нарушение этой работы (повреждение, хищение данных).

6.4. Для осуществления внешнего и внутреннего тестов на проникновение привлекаются лица, организационно не зависящие от Организации.

6.5. Тестирование системы ИБ должно проводиться не реже одного раза в год.

6.6. Проведение мероприятий по тестированию системы ИБ регламентировано Положением об управлении уязвимостями компонентов информационной системы ООО «Файнекс».

ГЛАВА 7
ТРЕБОВАНИЯ К ОБУЧЕНИЮ И ПРОВЕРКЕ ЗНАНИЙ РАБОТНИКОВ В ОБЛАСТИ ИБ

7.1. С работниками Организации, трудовые функции которых предполагают выполнение работы с использованием информационной системы Организации, проводятся мероприятия по обучению и проверке знаний в области ИБ.

7.2. Мероприятиями по обучению и проверке знаний в области ИБ являются:

вводные инструктажи;

плановые инструктажи;

доведение презентаций по отдельным направлениям обеспечения ИБ (противодействие фишингу, социальной инженерии и т.д.);

доведение сообщений о новых потенциальных угрозах, хакерских атаках и т.д. и рекомендациях по действиям персонала в конкретных условиях.

7.3. Вводные инструктажи проводятся с новыми работниками Организации перед их допуском к работе в информационной системе Организации.

В процессе вводных инструктажей до работников доводятся Правила информационной безопасности при работе пользователей в информационной системе ООО «Файнекс».

7.4. Плановые инструктажи проводятся со всеми работниками Организации в сроки, определенные директором Организации по предложению должностного лица, ответственного за системное администрирование и информационную безопасность Организации, но не реже чем один раз в год.

В процессе плановых инструктажей до работников доводятся Правила информационной безопасности при работе пользователей в информационной системе ООО «Файнекс», а также проводится проверка знаний работников в области ИБ по методике, утвержденной директором Организации.

7.5. Проведение вводных и плановых инструктажей регистрируется в журнале проведения инструктажей с росписью инструктируемого работника.

7.6. Мероприятия по обучению и проверке знаний работников Организации в области ИБ проводит должностное лицо, ответственное за системное администрирование и информационную безопасность Организации.

7.7. Обучение работника (работников), ответственного(-ых) за системное администрирование и информационную безопасность, осуществляется по отдельному плану.

ГЛАВА 8
ПРИНЯТИЕ РЕШЕНИЙ ПО УЛУЧШЕНИЮ СИСТЕМЫ ИБ

8.1. С целью достижения целей и задач по обеспечению эффективности системы ИБ, адекватного реагирования на возникающие угрозы, а также по результатам проведенных мониторинга, аудитов, тестирования и внутренних проверок системы ИБ, в систему ИБ должны вноситься необходимые изменения.

8.2. К изменениям системы ИБ относятся:

корректирующие действия, связанные с пересмотром настоящей Политики, а также положений, регламентов и инструкций, регламентирующих отдельные процессы обеспечения ИБ, порядок действий работников Организации;

внедрение новых средств обеспечения ИБ;

внедрение новых мер по защите информации и цифровых знаков (токенов);

внедрение новых мер, направленных на обеспечение бесперебойной работы информационной системы Организации;

внедрение новых процессов обеспечения ИБ.

8.3. Для принятия решений, связанных с внесением изменений в систему ИБ, рассматриваются:

материалы мониторинга и тестирования системы ИБ;

материалы анализа функционирования системы ИБ и применяемых защитных мер;

материалы анализа инцидентов ИБ;

появление новых информационных активов;

выявление новых угроз и уязвимостей ИБ;

изменения в оценке рисков нарушения ИБ;

успешные практики в области ИБ (собственные или других организаций);

изменения в законодательстве Республики Беларусь, актах Наблюдательного совета ПВТ;

изменения целей и задач Организации.

ГЛАВА 9
ПЛАНИРОВАНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ ИБ

9.1. Деятельность по обеспечению ИБ осуществляется в рамках годовых и текущих планов.

9.2. Годовое планирование обеспечения ИБ осуществляется в рамках годовых планов и должно включать:

мероприятия по совершенствованию правовой базы Организации в сфере ИБ;

мероприятия по организации процессов обеспечения ИБ;

мероприятия по повышению осведомленности работников Организации;

мероприятия по совершенствованию материально-технической базы системы ИБ;

мероприятия по обучению и повышению квалификации работников Организации, отвечающих за обеспечение ИБ.

9.3. Текущее планирование осуществляется с учетом выполнения мероприятий, предусмотренных годовым планом работ по обеспечению ИБ, а также новых задач, распоряжений должностных лиц Организации и изменений в текущей обстановке.

ГЛАВА 10
ОТЧЕТНЫЕ ДОКУМЕНТЫ ПО ВОПРОСАМ ИБ ОРГАНИЗАЦИИ

10.1. По результатам функционирования системы ИБ Организации лицом, ответственным за системное администрирование и информационную безопасность, разрабатываются и представляются следующие отчетные и информационные документы директору Организации:

ежемесячно отчет о состоянии ИБ предусматривающий: сведения о состоянии защищенности информационной системы Организации; анализе уровня рисков, которым эта система подвергается с учетом развития информационных технологий; фактах реализации указанных рисков в отчетном месяце и принятых по этим фактам мерах, уровне эффективности системы ИБ Организации и предложениях по ее совершенствованию;

отчеты по мониторингу и тестированию системы ИБ;

материалы служебных разбирательств по инцидентам ИБ;

иные документы по вопросам, входящим в компетенцию лица, ответственного за системное администрирование и информационную безопасность.

10.2. Планы, отчетные, информационно-справочные документы по вопросам обеспечения ИБ хранятся у лица, ответственного за системное администрирование и информационную безопасность.

ГЛАВА 11
ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ ОРГАНИЗАЦИИ ПО ОБЕСПЕЧЕНИЮ ИБ

11.1. Директор Организации:

определяет цели и задачи системы обеспечения ИБ;

утверждает ЛПА по вопросам организации ИБ Организации;

осуществляет руководство лицом (подразделением) ответственным за системное администрирование и информационную безопасность;

принимает решения о возможности и целесообразности использования технологий, повышающих риски нарушения ИБ;

принимает решения о приобретении аппаратно-программных средств для развития информационной системы и обеспечение ИБ.

11.2. Должностное лицо, ответственное за системное администрирование и информационную безопасность / Системный администратор:

обеспечивает функционирование информационной системы Организации;

вырабатывает предложения по развитию информационной системы Организации, внедрению передовых информационных технологий;

вырабатывает предложения по размещению компонентов информационной системы Организации в сторонних дата-центрах;

вырабатывает предложения по реализации функций администрирования и технической поддержки компонентов информационной системы Организации сторонними организациями;

участвует в разработке соглашений об уровне обслуживания (SLA, англ. Service Level Agreement);

обеспечивает реализацию организационных и технологических мер по обеспечению непрерывной работы и восстановлению работоспособности информационной системы Организации;

осуществляет анализ внешних и внутренних угроз ИБ, учет и оценку рисков нарушения ИБ в соответствии с Методикой управления риском нарушения информационной безопасности ООО «Файнекс», вырабатывает меры по их снижению;

вырабатывает предложения по реализации целей, задач и процессов обеспечения ИБ, внедрению наиболее эффективных методов, способов и средств защиты информации;

осуществляет классификацию и учет информационных активов, подлежащих защите, определяет угрозы указанным активам, вырабатывает меры по обеспечению защиты указанных активов;

осуществляет мониторинг системы ИБ;

организует проведение мероприятий по тестированию системы ИБ;

организует процесс управления портами ввода-вывода ПЭВМ и предоставления работникам Организации прав на использование внешних электронных носителей информации;

обеспечивает применение криптографических средств защиты информации и аутентификации участников информационного обмена;

организует предоставление доступа работникам Организации к информационным ресурсам Организации, осуществляет контроль предоставленных прав;

реализует мероприятия по использованию в Организации антивирусной защиты;

осуществляет разработку ЛПА по вопросам обеспечения ИБ и системного администрирования, осуществляет контроль выполнения требований указанных документов;

вносит предложения по обеспечению защиты сведений, относящихся к информации ограниченного распространения;

реализует мероприятия по повышению осведомленности и контролю знаний и навыков работников Организации по вопросам ИБ;

проводит разбирательства по инцидентам ИБ, и в случае необходимости выходит с предложениями по применению мер ответственности в отношении лиц, нарушивших правила ИБ;

составляет Отчетные документы по вопросам ИБ Организации в соответствии с Главой 10 настоящей Политики;

реализует иные функции в рамках имеющихся компетенций и предоставленных полномочий.

11.3. Работники Организации отвечают за исполнение правил ИБ на своем рабочем месте и обязаны:

знать перечни сведений ограниченного распространения Организации и правила обращения с указанными сведениями;

знать и соблюдать Правила информационной безопасности при работе пользователей в информационной системе ООО «Файнекс»;

сообщать директору и должностному лицу, ответственному за системное администрирование и информационную безопасность / системному администратору, о фактах нарушения правил обращения с информацией ограниченного распространения, правил работы в информационной системе Организации, а также об иных фактах, которые оказывают влияние на ИБ Организации.

11.4. Должностные лица и работники Организации имеют право вносить предложения по совершенствованию работы, связанной с выполнением обязанностей по обеспечению ИБ, предусмотренных настоящей Политикой.

11.5. Обязанности работников Организации по выполнению требований ИБ должны включаться в трудовые договоры (контракты) и (или) должностные инструкции работников.