ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«ВЫБОРГСКИЙ СУДОСТРОИТЕЛЬНЫЙ ЗАВОД»
(ПАО «ВСЗ»)

ПРИКАЗ

16.08.2024 № 203

Об утверждении Политики
информационной безопасности

В рамках реализации Концепции информационной безопасности АО «ОСК» и обществ Группы ОСК, в целях повышения эффективности работ по информационной безопасности в ПАО «ВСЗ»,

ПРИКАЗЫВАЮ:

1. Утвердить новую редакцию Политики информационной безопасности ПАО «ВСЗ» (далее - Политика ИБ).
2. Начальнику ОИБ Яшину А.Г. обеспечить размещение Политики ИБ в электронном виде в сети Общества по адресу: \Общие_папки\Подразделения\ОИБ.
3. Начальнику отдела маркетинга Ворошилову Н.В. обеспечить размещение Политики ИБ на официальном сайте предприятия.
4. Руководителям структурных подразделений учитывать положения Политики ИБ в своей основной деятельности.
5. Считать утратившим силу приказ ПАО «ВСЗ» от 24.01.2024 № 19 «Об утверждении Политики информационной безопасности».
6. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор С.Р. Черногубовский

№ проекта приказа: 1164

Утверждена приказом
генерального директора
от «16» 08 2024 № 203

Политика информационной безопасности ПАО «ВСЗ»

г. Выборг
2024 год

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в развитие Концепции информационной безопасности АО «ОСК» и обществ Группы ОСК (ОСК.КСМК 00.011-2024) с учетом требований законодательства Российской Федерации в области обеспечения ИБ.

1.2. Политика определяет позицию ПАО «ВСЗ» в отношении ИБ, основные цели, направления и меры по достижению целей и соблюдение принципов информационной безопасности в ходе производственной деятельности как организации оборонно-промышленного комплекса.

1.3. В рамках Политики принимается, что:

- информационные технологии играют важную роль в достижении бизнес-целей ПАО «ВСЗ»;
- в средствах информатизации ПАО «ВСЗ» циркулирует как открытая, общедоступная информация, так и информация ограниченного доступа;
- информация является ценным активом, требующим защиты независимо от форм её представления;
- информационная инфраструктура предприятия сталкивается с широким спектром угроз ИБ как внутреннего, так и внешнего характера, реализация которых может привести к различному ущербу (финансовые и репутационные потери, дезорганизация управленческой и производственной деятельности и т.д.);
- стратегической целью предприятия в области ИБ является внедрение и использование информационных технологий с учетом принимаемых рисков реализации угроз ИБ;
- стратегической задачей в области ИБ является создание системы обеспечения ИБ, основанной на методологии управления рисками и учитывающей актуальные угрозы бизнес-процессам.

1.4. Ключевыми объектами защиты являются: информационные системы и/или сервисы, а также объекты информатизации, предназначенные для обработки информации ограниченного доступа.

1.5. Положения настоящей Политики являются обязательным для работников предприятия, а также учитывается в отношениях ПАО «ВСЗ» со сторонними юридическими и физическими лицами.

1.6. Руководители структурных подразделений должны обеспечивать контроль соблюдения положений настоящей Политики.

2. Цели в области информационной безопасности

В области информационной безопасности устанавливаются следующие цели:

- соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;
- обеспечение безопасности корпоративных активов, включая материально-технические ценности, информационные ресурсы, бизнес-процессы;
- эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью;
- достижение экономически обоснованного применения мер по защите от реализации угроз информационной безопасности;
- повышение осведомленности работников в области рисков, связанных с используемыми информационными ресурсами;
- определение степени ответственности и обязанностей работников по обеспечению информационной безопасности.

3. Принципы обеспечения информационной безопасности

Система информационной безопасности ПАО «ВСЗ» должна быть основана на следующих ниже принципах.

Принцип системности: информационные ресурсы (активы) рассматриваются как взаимосвязанные и взаимовлияющие компоненты единой системы. Должно учитываться максимально возможное количество сценариев поведения системы в случае возникновения угроз информационной безопасности.

Принцип полноты (комплексности): для обеспечения информационной безопасности должен использоваться широкий спектр мер, методов и средств защиты, комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты.

Принцип эшелонированности: система обеспечения информационной безопасности должна стоиться таким образом, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

Принцип равнопрочности: эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки угроз либо недостаточности мер защиты.

Принцип непрерывности: обеспечение информационной безопасности является непрерывным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла активов.

Принцип разумной достаточности: руководство предприятия исходит из того, что создать «абсолютную» защиту невозможно, поэтому выбор средств защиты активов, адекватных реально существующим угрозам (т.е. обеспечивающих допустимый уровень возможного ущерба в случае реализации угроз), осуществляется на основе анализа рисков.

Принцип управляемости: должна существовать возможность мониторинга процессов, своевременного выявления нарушений информационной безопасности и принятия соответствующих мер.

Принцип персональной ответственности: ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

4. Область применения

Положения настоящей Политики распространяются на все информационные ресурсы (активы) предприятия и средства обработки информации. Соблюдение положений настоящей Политики обязательно для всех работников.

ПАО «ВСЗ» принадлежит на праве собственности вся деловая информация и вычислительные ресурсы, введенные в эксплуатацию в целях осуществления деятельности в соответствии с действующим законодательством и Уставом предприятия. Право собственности распространяется на приобретенное лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы, носители информации и сведения на этих носителях.

5. Ответственность за информационные ресурсы (активы)

В отношении всех собственных информационных ресурсов (активов), находящихся под контролем предприятия, а также активов, используемых для получения доступа к инфраструктуре предприятия, должна быть определена ответственность структурного подразделения или работника.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации, использовании за пределами предприятия, передача прав доступа сторонним лицам и организациям должна доводиться до сведения руководителей отдела информационных технологий и отдела информационной безопасности.

6. Контроль доступа к информационным системам

Все работы в помещениях предприятия выполняются только на средствах вычислительной техники, предоставленных предприятием.

Использование личных портативных компьютеров и внешних носителей информации (диски, flash-носители, и т.п.) возможно только по согласованию отдела информационных технологий и отдела информационной безопасности.

Конфиденциальность сведений, составляющих коммерческую тайну, обеспечивается применением мер, определяемых соответствующим организационно-распорядительным документом.

Руководители подразделений должны определять минимальные права доступа работников к информационным ресурсам в соответствии с их должностными обязанностями, расширение таких прав недопустимо.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени и пароля.

7. Доступ третьих лиц к информационным системам

Доступ третьих лиц к информационным ресурсам (активам) предприятия должен быть обусловлен производственной необходимостью. Такой порядок должен быть однозначно документально определен и контролируем.

7. Удаленный доступ

Работники должны получать право удаленного доступа к информационным ресурсам с учетом производственной необходимости.

Работникам, использующим в работе портативные компьютеры, принадлежащие предприятию, может быть предоставлен удаленный доступ к сетевым ресурсам в соответствии с правами в информационных системах.

Все компьютеры, подключаемые посредством удаленного доступа к информационным системам предприятия, должны иметь программное обеспечение антивирусной защиты, имеющее актуальное обновления сигнатур антивирусных баз.

Удаленный доступ к информационным системам контрагентов должен быть организован с применением тех мер и средств защиты информации, которые определены владельцами таких информационных систем.

8. Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для деятельности, противоречащей законодательству Российской Федерации.

Предприятие имеет право контролировать содержание всего трафика, как входящего, так и исходящего.

9. Защита оборудования

Работники должны постоянно помнить о необходимости обеспечения безопасности оборудования, на котором хранится принадлежащая предприятию информация.

Изменение конфигурации аппаратного и программного обеспечения должно производиться только отделом информационных технологий или отделом информационной безопасности.

10. Аппаратное обеспечение

Средства вычислительной техники, предоставленные предприятием, являются его собственностью и предназначено для использования исключительно в производственных целях.

Работники, получившие в пользование портативный компьютер, обязаны принять надлежащие меры по обеспечению его сохранности.

Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере средств вычислительной техники.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства

не относятся к числу устройств, имеющих надежные механизмы защиты данных. Хранение конфиденциальной информации на таких устройствах не рекомендуется.

Порты передачи данных, в том числе CD дисководы в стационарных компьютерах блокируются, за исключением случаев, когда запись информации согласована отделом информационной безопасности.

11. Программное обеспечение

Все программное обеспечение, устанавливаемое на предоставленных средствах вычислительной техники, должно использоваться исключительно в производственных целях.

Самостоятельная установка работником программного обеспечения не предусматривается.

12. Использование электронной почты

Содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других работников и не препятствует бизнес деятельности.

Для обмена документами и информацией с контрагентами должен использоваться только принадлежащий предприятию адрес электронной почты (name@vsy.ru).

13. Защита и сохранность данных

Ответственность за сохранность данных лежит на работниках. Специалисты отдела информационных технологий оказывают работникам содействие в проведении резервного копирования данных.

Только специалисты отдела информационных технологий на основании заявок руководителей подразделений имеют право создавать и удалять совместно используемые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

Работники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, к которым они имеют санкционированный доступ.

14. Разработка систем и управление внесением изменений

Все процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны руководителями отделов информационных технологий и информационной безопасности.

Начальник отдела информационной безопасности  А.Г. Яшин