УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТАНДАРТ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТАНДАРТ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

[ИБ-201]

(версия 1.2)

2018 г.

Оглавление

1. Введение

Информационная инфраструктура ООО «Сатурн» (далее – Компания) состоит из разнообразных компонентов, каждый из которых выполняет свою функцию. Для обеспечения информационной безопасности Компании в целом, необходимо обеспечение безопасности каждого из компонентов. Одной из наиболее важных составляющих системы защиты является защита автоматизированных рабочих мест (АРМ) пользователей, на которых ежедневно осуществляется обработка, передача, хранение конфиденциальной информации Компании. Так же необходимо учитывать возможное влияние состояния отдельного рабочего места сотрудника на информационные системы и другие составляющие ИТ-инфраструктуры Компании.

Ввиду того, что количество защищаемых АРМ пользователей велико, а перечень программных средств и информации, обрабатываемой с их помощью, включает в себя всю информацию, циркулирующую в рамках Компании, существует необходимость стандартизации рабочих мест и классификации защитных мер, применяемых к каждому АРМ.

С учетом оценок состояния информационной безопасности и возможностей пользователей, к основным рискам на АРМ относятся:

- Юридические и репутационные риски;
- Не санкционированный и(или) не контролируемый доступ;
- Компьютерные атаки на ИТ-инфраструктуру группы компаний;
- Нарушение устойчивости и непрерывности бизнес-процессов;
- Преднамеренные и случайные утечки информации.

Юридические и репутационные риски могут быть вызваны:

- возможностью пользователей устанавливать на АРМ компании любое, в том числе нелицензионное программное обеспечение. Претензии будут выдвигаться к компании, а не к конкретному нарушителю.
- отсутствием реализации политик, обеспечивающих выполнение требований федерального законодательства по защите персональных данных.
- отсутствием ограничений по доступу к ресурсам корпоративной сети и Интернет (нет ограничений по используемым сервисам, объему трафика и его содержанию, отсутствует авторизация подключений устройств к корпоративной сети). При этом риск возникает не только по причине возможной загрузки нелицензионного контента, но и в связи с возможностью предоставления его другим пользователям Интернет.

Отсутствие должного контроля и ограничения использования Интернет может привести к использованию ИТ ресурсов компании для рассылки спама, функционирования bot-net сетей, DDOS атак и т.п. Что в свою очередь может привести не только к юридическим последствиям, но и включению компании в «черные» списки и потере репутации.

Не санкционированный и(или) не контролируемый удаленный доступ к ИТ ресурсам компании могут быть вызваны:

- использованием простой не многофакторной системы аутентификации;
- использованием сотрудниками средств удаленного доступа и администрирования.

Компьютерные атаки на ИТ-инфраструктуру Компании могут быть вызваны:

- отсутствием ограничений по доступу в Интернет;

- целенаправленной деятельностью легальных и/или привилегированных пользователей;
- низким уровнем эффективности средств защиты.

Нарушение устойчивости и непрерывности бизнес процессов могут быть вызваны:

- отсутствием ограничений по доступу в Интернет;
- наличием у сотрудников возможности установки программного обеспечения на своих рабочих местах. Такое программное обеспечение может содержать уязвимости, которые могут использоваться злоумышленниками для получения контроля над АРМ пользователей и элементами ИТ-инфраструктуры компании.
- наличием у сотрудников возможности установки нелегальных технических средств которые:
  - порождают дополнительную нагрузку на IT ресурсы компании;
  - повышают вероятность сбоев;
  - порождают новые не контролируемые каналы утечки данных;
  - в случае наличия уязвимостей, дают дополнительные возможности вероятным злоумышленникам использовать их для атак на ИТ-инфраструктуру компании.
- воздействие вирусов и другого вредоносного программного обеспечения из-за недостаточного контроля за переносными устройствами хранения данных и каналами передачи данных и т.п.

Преднамеренные и случайные утечки критических для бизнеса компаний данных могут быть вызваны:

- неконтролируемым использованием переносных устройств хранения данных;
- наличием не контролируемых каналов передачи информации.

Рекомендации по минимизации рисков, а также требования законодательства РФ о персональных данных:

- обеспечение управления и контроля доступов пользователей к ИТ-ресурсам Компании, поддержание доступов в актуальном состоянии в соответствии с производственными необходимостями пользователей;
- обеспечение сегментации информационной системы в зависимости от функциональных обязанностей групп/отделов пользователей;
- обеспечение антивирусной защиты АРМ пользователей с применением централизованного управления политиками и получением отчетов о вирусных заражениях в корпоративной сети;
- обеспечение защиты от утечек конфиденциальной информации с применением внешних носителей данных, а также иных каналов передачи информации;
- обеспечение резервирования критичной информации на внешние носители информации;
- обеспечение минимизации прав пользователей до необходимых для выполнения ими функциональных обязанностей;
- контроль и ограничение доступа в Интернет для всех сотрудников до минимально необходимых наборов служб - например, http, https, skype.
- усиление аутентификации системы удаленного доступа, минимум, одним фактором (сертификат, OTP и т.д.);

- запрет использования средств удаленного администрирования непрофильными сотрудниками.

2. Меры по минимизации ключевых рисков на АРМ

2.1. Технические меры, направленные на минимизацию ключевых угроз на АРМ

Таблица 1. Технические меры.

№ п.п.	Ключевые риски	Защитные меры
1.	Юридические и репутационные риски	• включение в ИТ-инфраструктуру системы контроля и управления траффиком Интернет; • включение в ИТ-инфраструктуру системы контроля и управления корпоративной электронной почты; • реализация требований федерального законодательства по обеспечению безопасной обработки персональных данных; • реализация требований электронных торговых площадок, предъявляемых для участников электронных торгов (т.к. ЭТП АСТ ГОЗ, Сбербанк-АСТ и т.п.) • реализация требований Европейского регламента по защите персональных данных 2016/679 от 27 апреля 2016 г.
2.	Не санкционированный и(или) не контролируемый доступ	• включение в ИТ-инфраструктуру системы авторизации сетевых устройств; • включение в ИТ-инфраструктуру системы многофакторной аутентификации; • включение в ИТ-инфраструктуру системы учета, контроля и ограничения использования на АРМ сотрудников незарегистрированных носителей и иных технических средств; • внедрение системы оценки защищенности информационных систем и информационной инфраструктуры предприятия; • включение в ИТ-инфраструктуру корпоративных антивирусных средств; • включение в ИТ-инфраструктуру системы контроля и управления траффиком Интернет; • внедрение систем межсетевого экранирования, обнаружения и предотвращения вторжений; • внедрение системы конфиденциального электронного документооборота (СКЭД); • включение в ИТ-инфраструктуру системы защищенного удаленного доступа к

№ п.п.	Ключевые риски	Защитные меры
		виртуальным рабочим столам, сервисам или приложениям; • включение в ИТ-инфраструктуру системы шифрования носителей на переносных персональных компьютерах.
3.	Компьютерные атаки на ИТ-инфраструктуру группы компаний	• реализация ограничения и контроля доступа к сети Интернет. • обеспечение антивирусной защиты АРМ с применением централизованного управления средством защиты.
4.	Нарушение устойчивости и непрерывности бизнес-процессов	• включение в ИТ-инфраструктуру системы контроля и управления траффиком Интернет; • внедрение систем межсетевого экранирования, обнаружения и предотвращения вторжений; • включение в ИТ-инфраструктуру системы контроля и управления корпоративной электронной почты; • внедрение системы конфиденциального электронного документооборота (СКЭД); • включение в ИТ-инфраструктуру корпоративных антивирусных средств; • включение в ИТ-инфраструктуру системы авторизации сетевых устройств; • включение в ИТ-инфраструктуру системы многофакторной аутентификации.
5.	Преднамеренные и случайные утечки информации	• включение в ИТ-инфраструктуру системы учета, контроля и ограничения использования на АРМ сотрудников незарегистрированных носителей и иных технических средств; • включение в ИТ-инфраструктуру системы контроля и управления траффиком Интернет; • внедрение систем межсетевого экранирования, обнаружения и предотвращения вторжений; • включение в ИТ-инфраструктуру системы контроля и управления корпоративной электронной почты; • внедрение системы конфиденциального электронного документооборота (СКЭД); • включение в ИТ-инфраструктуру системы защищенного удаленного доступа к виртуальным рабочим столам, сервисам или приложениям; • включение в ИТ-инфраструктуру системы шифрования носителей, включая

№ п.п.	Ключевые риски	Защитные меры
		физические и логические диски на переносных персональных компьютерах; • расширение функционала корпоративной DLP системы; • обеспечение защищенных цифровых каналов связи между территориально распределенными подразделениями; • развертывание системы аудита изменений в ИТ-инфраструктуре ключевых информационных систем.

2.2. Перечень технических мер, направленных на минимизацию рисков на АРМ

2.2.1. Применение средств контроля работы в локальной сети

2.2.1.1. АРМ допущен в локальную сеть, пройдя процедуру аутентификации по протоколу 802.1x;

2.2.1.2. АРМ заведен в отдельный VLAN, обеспеченный защитой от внешних сетевых атак, а также средствами контроля сетевого трафика;

2.2.1.3. АРМ с выключенными средствами RDP;

2.2.1.4. АРМ с отключенными расшаренными ресурсами;

2.2.1.5. АРМ с включенным доступом VPN.

2.2.2. Применение средств контроля и защиты АРМ

2.2.2.1. АРМ с отключенными USB-портами и партами, позволяющими подключение внешних устройств;

2.2.2.2. АРМ с программным обеспечением управления доступом к съемным устройствам;

2.2.2.3. АРМ находится под контролем средства обеспечения безопасности от утечек конфиденциальной информации на локальных жестких дисках;

2.2.2.4. АРМ находится под контролем средства мониторинга и инвентаризации изменений программной и аппаратной части;

2.2.2.5. АРМ с программным обеспечением контроля за утечками конфиденциальной информации по различным каналам связи;

2.2.2.6. АРМ с установленным корпоративным средством обеспечения антивирусной защиты;

2.2.2.7. АРМ с применением шифрования носителей информации;

2.2.2.8. Использование защищенных внешних носителей с аппаратным шифрованием информации;

2.2.3. Дополнительные меры защиты

2.2.3.1. На АРМ реализована политика парольной защиты;

2.2.3.2. На АРМ реализована двухфакторная система авторизации;

2.2.3.3. Вход на АРМ реализован с применением аппаратного ключа авторизации;

2.2.3.4. Исключение прав локального администратора у пользователя АРМ;

2.2.3.5. АРМ не содержит ПО, не предназначенного для выполнения должностных обязанностей;

2.2.3.6. Резервное копирование информации, содержащейся на АРМ;

2.2.3.7. На АРМ реализована своевременная установка обновлений системного и прикладного ПО;

2.2.3.8. Технические средства АРМ опломбированы(наклейки).

2.2.4. При организации доступа к сети Интернет

2.2.4.1. АРМ без доступа в Интернет;

2.2.4.2. АРМ с доступом в Интернет с применением средств контроля и фильтрации;

2.2.4.3. АРМ с доступом в Интернет с помощью терминального подключения с применением средств контроля и фильтрации.

2.3. Перечень организационных мер, направленных на минимизацию рисков на АРМ

- Пользователям запрещено использование с рабочих компьютеров любых внешних файлообменных сервисов и ПО (DropBox, Google Drive, Yandex Disk и т.п.).
- Пользователям запрещено хранение документации по проектам, иной информации в электронном виде, являющейся собственностью Компании или переданной заказчиками, исполнителями, партнерами в адрес Компании на IT-ресурсах за пределами ИТ-инфраструктуры Компании.
- Пользователям запрещено использование торрент-клиентов и прочего подобного ПО, построенного с использованием P2P-сетей.
- Пользователям запрещено использование любых способов организации удаленного доступа к IT-ресурсам Компании (TeamViewer и т.п.) за исключением предоставляемого IT-департаментом Компании VPN.
- Пользователям запрещено предоставление неконтролируемого общего доступа к папкам на рабочих станциях пользователей.
- Для создания резервных копий служебной информации, при необходимости, сотрудникам необходимо использовать сервисы, предоставляемые IT-департаментом Компании («newstorage»).
- Пользователям запрещено использование внешних мессенджеров (whatsapp, telegram и т.п.) и иных внешних сервисов для обмена служебной информацией и построения рабочих/бизнес/производственных процессов.
- Пользователям запрещено использование сервисов мгновенного обмена сообщениями для решения служебных задач.
- Разработана и опубликована Политика Оператора в отношении персональных данных.
- Разработано и введено в действие Положение об обработке персональных данных, регламентирующее правила хранения, разграничение доступа, правила обработки и передачи персональных данных работников, а также ответственность вовлеченных в процесс обработки персональных данных.
- Для ограничения доступа посторонних на территорию Компании и в помещения, в которых расположены АРМ, используется система контроля и управления доступом, контроллеры управления доступом, считыватели и электромагнитные замки.
- АРМ должен быть размещен в пределах контролируемой зоны.

- Проход на территорию Компании и в охраняемые помещения контролируется с использованием систем видеонаблюдения.
- На территории Компании соблюдаются меры противопожарной безопасности.
- Запрещено самостоятельно вскрывать технические средства и вносить изменения в состав АРМ.

Перечень организационных мер должен поддерживаться техническими мерами.

3. Организационно-распорядительная документация

В целях закрепления требований Компании по защите информации, а также создания возможности ознакомления с ними уполномоченных сотрудников разработана организационно-распорядительная документация (ОРД) по безопасности, регламентирующая использование АРМ, сетевых ресурсов, включая использование сети Интернет и систему корпоративной электронной почты, использование внешних средств хранения информации и т.д.

3.1.1. Состав ОРД в части использования ИТ-ресурсов Компании

- Приказ Генерального Директора от ***** 2018 № *****;
- Политика управления парольной защитой;
- Политика предоставления доступа к ИТ-ресурсам;
- Инструкция по учету, хранению и выдаче средств хранения информации;
- Инструкция по организации парольной защиты в информационных системах и системах обработки информации;
- ***

3.1.2. Состав ОРД в части защиты персональных данных

- Политика в отношении обработки персональных данных;
- Публичная политика обработки персональных данных;
- Регламент предоставления доступа к персональным данным;
- Регламент обмена персональными данными с третьими лицами;
- Регламент обращения с машинными носителями персональных данных;
- Регламент доступа в помещения, в которых ведется обработка персональных данных;
- Положение об обеспечении безопасности персональных данных;
- ***

4. Порядок реализации мер

Меры по защите информации распространяются на пользователей дифференцированно, в зависимости от производственных необходимостей, технических возможностей и экономической целесообразности принятия тех или иных мер.

В общем случае, порядок выбора и реализации мер состоит из следующих шагов:

- Сбор информации о должностных обязанностях сотрудника.
- Консультация с руководителем сотрудника о необходимости наличия у пользователя доступов к ресурсам и функциям ИТ инфраструктуры Компании.
- Проработка оптимальной комбинации защитных мер, исходя из принципа назначения минимально необходимых прав доступа.
- В зависимости от выбранных технических мер осуществляется установка и настройка СрЗИ на АРМ пользователя, при необходимости, проводится обучение

пользователя, присваиваются соответствующие права доступа.

- В зависимости от наличия доступа к определенным видам информации, пользователь ознакамливается с соответствующими организационно-распорядительными документами.
- Сотрудник приступает к выполнению должностных обязанностей с учетом реализованных мер по защите информации.

5. Контроль и учет

Контроль и учет реализации защитных мер ведется силами Департамента по безопасности и информационным технологиям.

Учет ведется в виде электронного реестра с указанием отдела сотрудника, реализованных технических мер, полученных доступов и т.п.

Контроль за соответствием АРМ требованиям настоящего Стандарта осуществляется с применением консолей администрирования СрЗИ, используемых в Компании, а также с помощью иного специального ПО.