Тема 8

Информационная безопасность автоматизированных систем управления технологическими процессами

Содержание темы

- Обзор инцидентов в сфере информационной безопасности.
- Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.
- Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».
- Особенности функциональной безопасности.
- Защита информации в АСУ ТП.

КВОИ

Указ Президента Республики Беларусь
25 октября 2011 г. № 486

«О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»

КВОИ

Критически важный объект информатизации – это объект информатизации, который:

1) обеспечивает функционирование **экологически опасных** и (или) **социально значимых** производств и (или) **технологических процессов**, нарушение штатного режима которых может привести к **чрезвычайной ситуации техногенного характера**;

КВОИ

Критически важный объект информатизации – это объект информатизации, который:

2) осуществляет функции **информационной системы**, нарушение (прекращение) функционирования которой может привести к **значительным негативным последствиям для национальной безопасности** в политической, экономической, социальной, информационной, экологической, иных сферах;

КВОИ

Критически важный объект информатизации – это объект информатизации, который:

3) обеспечивает предоставление значительного объема **информационных услуг**, частичное или полное прекращение оказания которых может привести к **значительным негативным последствиям для национальной безопасности** в политической, экономической, социальной, информационной, экологической, иных сферах.

КВОИ

Указ Президента Республики Беларусь
9 ноября 2010 г. № 575

«**Об утверждении Концепции национальной безопасности Республики Беларусь**»

Изменения и дополнения:

Указ Президента Республики Беларусь от 30 декабря 2011 г. № 621

КВОИ

1) Основными **национальными интересами** в информационной сфере являются: …**обеспечение надежности и устойчивости функционирования критически важных объектов информатизации**

Глава 2 – Национальные интересы

КВОИ

2) Основными потенциальными либо реально существующими **угрозами национальной безопасности** являются: …**нарушение функционирования критически важных объектов информатизации**

Глава 4 – Основные угрозы национальной безопасности

КВОИ

3) В информационной сфере **внутренними источниками угроз национальной безопасности** являются:
…несовершенство системы обеспечения безопасности критически важных объектов информатизации

Глава 5 – Внутренние источники угроз национальной безопасности

Постановление СМ РБ № 293 от 30.03.2012

Постановление Совета Министров
Республики Беларусь
30 марта 2012 г. N 293

«О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»

Постановление СМ РБ № 293 от 30.03.2012

Отраслевые критерии:

1) Критерий **экологической опасности** производства, функционирование которого обеспечивается объектом информатизации;

2) Критерий **социальной значимости производства**, функционирование которого обеспечивается объектом информатизации;

3) Критерий важности объекта информатизации, осуществляющего функции **информационной системы**;

4) Критерий важности объекта информатизации, обеспечивающего **предоставление значительного объема информационных услуг.**

Постановление СМ РБ № 293 от 30.03.2012

Примерный перечень показателей уровня ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае возникновения угроз различного характера в отношении объекта информатизации (его составляющих элементов)

Показатели ущерба	Уровень ущерба		
	умеренный	высокий	катастрофический
1. Ущерб здоровью людей Количество людей (КЛ), подвергшихся воздействию	Серьезные повреждения требующие госпитализации или многократного обращения за медицинской помощью 100 <= КЛ <= 1000	Повреждения с угрозой для жизни, вызывающие необходимость госпитализации 1000 <= КЛ <= 10000	Гибель людей или многочисленные повреждения с угрозой для жизни КЛ > 10000

Постановление СМ РБ № 293 от 30.03.2012

Показатели ущерба	Уровень ущерба		
	умеренный	высокий	Катастрофичес-кий
2. Вред, причиненный окружающей среде.	Вредное воздействие на окружающую среду носит локальный характер в пределах территории объекта, функционирование которого обеспечивается объектом информатизации	Вредное воздействие на окружающую среду выходит за границы территории объекта, функционирование которого обеспечивается объектом информатизации	Вредное воздействие на окружающую среду имеет трансграничный характер
3. Снижение качества выполнения основных процессов (заданных целевых функций)	Снижение эффективности выполнении процессов, функций (задач). Невыполнение одной и более основных функций	Ухудшение управляемости объекта, снижение качества обслуживания, не совместимое с установленными требованиями качества	Нарушение основных процессов, срыв задач управления-прекращение функционирования объекта

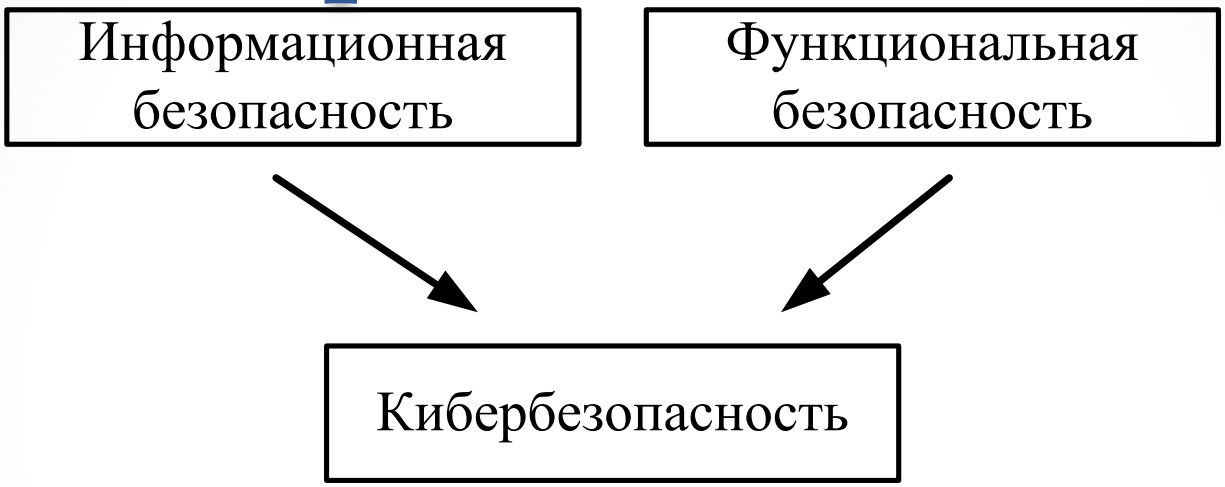
Постановление СМ РБ № 293 от 30.03.2012

Показатели ущерба	Уровень ущерба		
	умеренный	высокий	Катастрофичес-кий
4. Снижение качества выполняемых процессов смежных (зависимых) объектов	Умеренное воздействие на важные процессы других объектов в пределах одного района или области (региональный уровень)	Существенное воздействие на функционирование или разрушение других объектов в пределах территории государства (республиканский государственный уровень)	Воздействие на объекты других Государств (трансграничный уровень)
5. Экономический ущерб (ЭУ), в процентах от бюджета административно-территориальной единицы по месту нахождения (регистрации) субъекта хозяйствования	2,5 < ЭУ <= 10	10 < ЭУ <= 25	ЭУ > 25

Функциональная безопасность

Информационная безопасность	Функциональная безопасность
Совокупность таких условий функционирования системы управления, при которых обеспечивается конфиденциальность целостность и доступность содержащейся в ней информации	Совокупность таких условий функционирования системы управления, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного функционирования системы

Кибербезопасность



Совокупность политик и действий, которые должны быть предприняты для защиты критически важных объектов от деструктивных информационных воздействий (несанкционированный доступ, компьютерная атака, программно-аппаратные закладки, недекларированные возможности, искажение, кража, уничтожение информации), направленных на нарушение штатного функционирования этих систем

Сомнения владельца (заказчика)

Квалификация в сфере обеспечения ИБ и ФБ

Разработчик

???

Модель нарушителя

Злоумышленник

Квалификация в сфере железнодорожных систем

Аккредитованные эксперты в области ЗИ

Система управления

Уязвимости системы, серийного «железа» и ПО, на базе которого она организована

Владелец (заказчик)

ИБ – информационная безопасность;
ФБ – функциональная безопасность

Условия максимально безопасной эксплуатации систем управления на железнодорожном транспорте

ОАЦ при Президенте Республики Беларусь

Оценка ИБ

Система управления

Нарушение ИБ

Нарушение ФБ

Злоумышленник

Эксплуатация

Надежное сопровождение

Оценка ИБ и ФБ

Нарушение ИБ и ФБ

Владелец (заказчик)

Разработчик

Аккредитованный специалист в области ЗИ и СУнаЖДТ

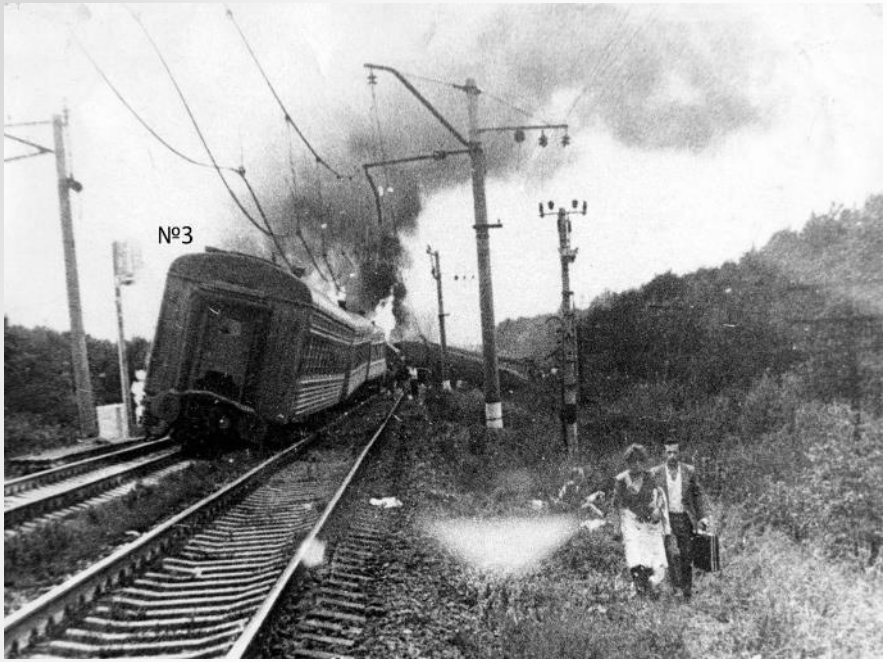
«Свой» злоумышленник

Фактические действия

Возможные действия

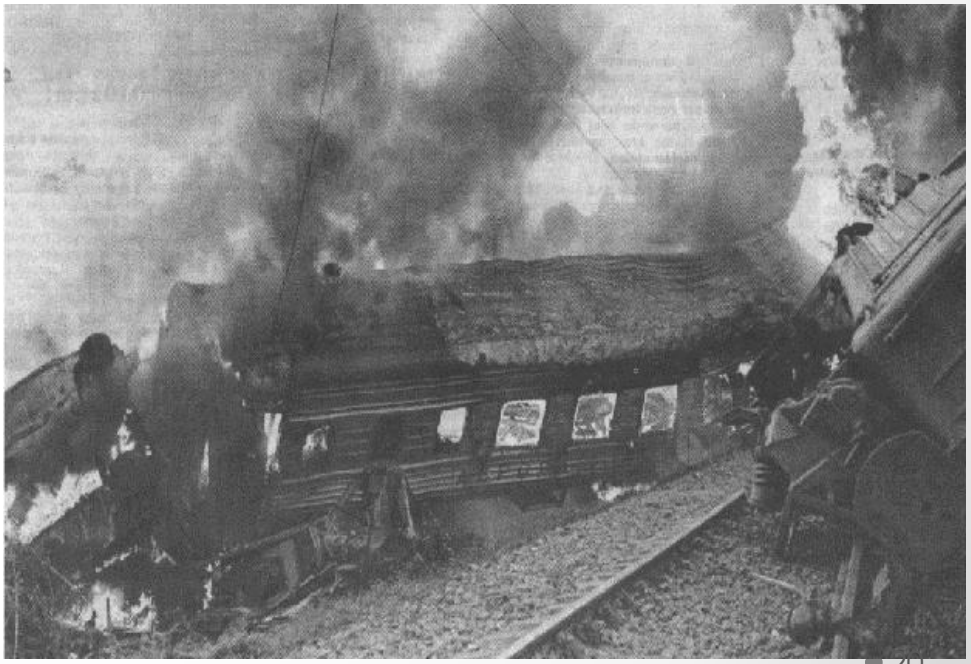
ЗИ – защита информации;
ИБ – информационная безопасность;
СУнаЖДТ – система управления на железнодорожном транспорте;
ОАЦ – Оперативно-аналитический центр;
ФБ – функциональная безопасность.

«Одна команда»



Крушение пассажирского поезда «Аврора» на перегоне Березайка – Поплавенец 16 августа 1988 года.

В результате схода с рельсов всех вагонов поезда 31 человек погиб, более 100 пострадали, движение на участке было остановлено более чем на 15 часов.



Крушение пассажирского поезда «Юрмала» 3 марта 1992 года на разъезде Подсосенка участка Великие Луки – Ржев Октябрьской железной дороги. Пассажирский поезд столкнулся со встречным грузовым составом. В результате столкновения поездов 43 человека погибли, 108 получили травмы. Допущен перерыв движения поездов на участке 15 часов 30 минут.

25 апреля 2005 года в Японии скоростной поезд отставал от графика, поэтому машинист решил рискнуть и превысил скорость до 116 км/ч на опасном повороте, где максимально разрешенной скоростью было 70 км/ч. В результате поезд сошел с рельс и врезался в здание паркинга недалеко от станции Амагасаки. Два первых вагона от удара были буквально расплющены, остальные тоже оказались сильно поврежденными. В поезде находилось около 700 человек, из них 107 погибло, 562 получили ранения.

Крушение поезда в Сантьяго-де-Компостела 24 июля 2013 года. Высокоскоростной поезд Alvia подъезжал к станции Сантьяго-де-Компостела, когда все 8 вагонов поезда сошли с рельсов и перевернулись. Причиной катастрофы стало более чем двукратное превышение скорости состава при прохождении кривого участка пути. 79 человек погибли и около 140 получили ранения.